www.sapientia.uji.es | 170

Elementos de Matemática discreta

Julio José Moyano Fernández



Col·lecció «Sapientia», núm. 170

ELEMENTOS DE MATEMÁTICA DISCRETA

Julio José Moyano Fernández

Departament de Matemàtiques

■ Código de la asignatura: EIMT1006



Edita: Publicacions de la Universitat Jaume I. Servei de Comunicació i Publicacions
Campus del Riu Sec. Edifici Rectorat i Serveis Centrals. 12071 Castelló de la Plana
http://www.tenda.uji.es e-mail: publicacions@uji.es

Colección Sapientia 170
www.sapientia.uji.es
Primera edición, 2021

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170



Publicacions de la Universitat Jaume I es miembro de la UNE, lo que garantiza la difusión y comercialización de sus publicaciones a nivel nacional e internacional. www.une.es.



Este libro, de contenido científico, ha estado evaluado por personas expertas externas a la Universitat Jaume I, mediante el método denominado revisión por iguales, doble ciego.

ÍNDICE

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Prefacio

El presente texto se propone como notas ampliadas de la asignatura “Matemáticas II” que imparto en el segundo semestre del primer curso de los grados en Matemática Computacional y en Ingeniería Informática ofertados en la Universitat Jaume I de Castellón de la Plana. El objetivo del curso es la adquisición por parte del alumno de los conceptos fundamentales de teoría naïve de conjuntos, lógica booleana, aritmética de los números enteros y las técnicas básicas en combinatoria enumerativa y combinatoria existencial constructiva.

Por otra parte, con estas notas me propongo evitar al alumno la tediosa copia de la lección directamente de la pizarra. Estando convencido del uso de la misma como mejor medio de transmisión de discusiones y conocimientos matemáticos, la tenencia a priori de los apuntes por el estudiante fluidifica la comunicación docente-alumno y facilita que el estudiante reflexione ya en el aula sobre los conceptos que se explican, en lugar de dedicar ese valiosísimo tiempo en la irreflexiva copia manuscrita de la lección dictada, con sus aciertos y errores.

El presente manuscrito bebe principalmente de tres fuentes, a saber: los primeros capítulos de mis notas “Mathematik für Anwender I”, curso que impartí en la Universidad de Osnabrück (Alemania) en el semestre de verano de 2013, en las notas realizadas por el Prof. Dr. Winfried Bruns para la asignatura “Elemente der diskreten Mathematik” impartida en el Semestre de invierno 2011/12 en la Universidad de Osnabrück, así como en las notas que tomé —siendo alumno de cuarto curso de la licenciatura en Matemáticas en la Universidad de Valladolid— en la asignatura “Métodos, modelos y estructuras discretas” impartida en aquel cuatrimestre de transición entre los años 2001 y 2002 por la Prof. Dr. Ana Núñez Jiménez.

Julio José Moyano Fernández

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Innovación educativa

La redacción de este manual se enmarca en las dinámicas que se han ido sucediendo y se suceden en el seno del Grupo d’Innovació Educativa–GIE

IEALYGEO — Investigación Educativa en la enseñanza-aprendizaje del Álgebra y la Geometría,

de la Universitat Jaume I, y en particular en la Acció d’innovació 3846 correspondiente al año 2020, así como en el Projecte d’innovació educativa 3955 concedido en el año 2021.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Antes de comenzar...

Las páginas que se suceden a continuación son los contenidos teóricos, expuestos en forma de apuntes ligeramente ampliados, de una asignatura estándar de Matemática discreta que se imparta en un primer curso universitario. Puede que llamen la atención dos hechos:

(a) Que haya tantos capítulos y que se llamen así, *capítulos*: efectivamente hay muchos, pero son cortos. Con ello se quiere alcanzar una especie de éxito psicológico al terminar cada uno, es decir, que el estudiante se sienta satisfecho de haber terminado una unidad; al ser unidades cortas se potencia esta sensación. El nombre de *capítulo* quiere dar a entender que no son unidades al azar recogidas en un libro, sino que existe una cierta coherencia interna entre uno y el siguiente, como en una novela.

(b) Que no haya ejercicios, ni propuestos ni resueltos: a lo largo del texto se intercalan numerosos ejemplos, pero es verdad que no se proponen ejercicios. Esto es en parte porque se pretendía redactar un manual teórico, en parte porque se tiene la intención de hacer una publicación semejante pero con contenidos estrictamente prácticos. No obstante, en las referencias que se proponen al final de cada capítulo (y que se recopilan de nuevo al final del libro) aparecen obras con muchas sugerencias prácticas.

La dificultad obvia de esta asignatura es *de expresión*, podríamos decir: una queja habitual entre ciertos grupos de estudiantes es la dificultad que encuentran en el lenguaje utilizado para transmitir el mensaje (las matemáticas). Lamentablemente para ellos, pero afortunadamente en sentido global, este lenguaje se usa a propósito: es un objetivo de esta asignatura enfrentar al estudiantado neófito en matemáticas con el lenguaje matemático que se usará de manera común a lo largo de su futuro, en la universidad y cada vez que tome un artículo o manual científico que involucre descripciones matemáticas. El alumnado tiene que pensar que esto no se concibe así para perjudicarle, y que además sucede en cualquier universidad del mundo a un nivel equivalente. En este sentido, y en otros, quizás haya que adoptar la postura que de vez en cuando me recuerda una buena amiga, desmitificando el velo de la ignorancia: no saber es siempre peor que saber.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Conocimientos previos

Al lector o lectora de estas notas se le supone conocer:

- ◇ que $\mathbb{N}$ denota la reunión de todos los números naturales, incluyendo el 0;
- ◇ que $\mathbb{Z}$ denota la reunión de todos los números enteros, que son los naturales y los naturales con signo negativo;
- ◇ que $\mathbb{Q}$ denota la reunión de todos los números racionales, que son las fracciones con *numerador* un número entero y *denominador* un número entero distinto de 0;
- ◇ que $\mathbb{R}$ denota la reunión de todos los números reales —aunque estos nunca le fueron definidos y en este curso tampoco sucederá;
- ◇ las operaciones básicas de números naturales, enteros, racionales y reales, con las que ya se ha familiarizado en la matemática preuniversitaria;
- ◇ los símbolos "$=$" (igual que), "$<$" (menor que), "$\leq$" (menor o igual que), "$>$" (mayor que) y "$\geq$" (mayor o igual que), referidos a números de los tipos anteriores, que además maneja con soltura;
- ◇ lo que es un número (natural) par y un número (natural) impar; en particular, que 0 es un número par;
- ◇ el significado intuitivo de la propiedad conmutativa (lo que popularmente se enuncia como "el orden de los factores no altera el producto");
- ◇ solamente para algún ejemplo puntual, los rudimentos del cálculo matricial y del cálculo infinitesimal.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Capítulo 1. Lógica proposicional: un primer contacto

Si tenemos la imagen de un matemático como una especie de ordenador que transforma afirmaciones en teoremas,[1] podemos entonces preguntarnos por el metalenguaje que entiende. Este no es otro que la teoría del razonamiento coherente, esto es, la lógica.

Con ayuda de reglas de inferencia bien definidas, los matemáticos *demuestran* la validez de sus afirmaciones —esto es, las transforman en teoremas— continuamente. Comprender el proceso subyacente es tarea de la lógica.

Como punto de partida de nuestro curso, y como herramienta necesaria para poder avanzar en los primeros conceptos matemáticos, presentamos una introducción, necesariamente básica, a los primeros conceptos de la lógica proposicional, que es la parte de la lógica que se ocupa del estudio de las proposiciones y su interrelación a través de conectores lógicos.

Proposiciones. Una *proposición* es una frase descriptiva, como "el edificio es bonito", "la nieve es blanca". Preguntas, órdenes y otras expresiones lingüísticas similares no son proposiciones. He aquí algunos ejemplos de expresiones que *no* son proposiciones:

* $\emptyset$;
* $67+78$;
* ¡Juan, ven enseguida!
* El conjunto de los números enteros.

El punto de partida son las proposiciones *simples*, como por ejemplo "la chica es alta"; con ellas se pueden formar proposiciones más elaboradas o *compuestas*, como "la chica es alta y su hermano también".

La lógica proposicional se marca como objetivo la coherencia de las relaciones entre proposiciones; para ello empieza fijando unas proposiciones que son las reglas del juego: son los *axiomas*. La expresión "axioma" es en realidad polisémica; con ella se puede querer designar:

(i) una afirmación fundamental que se comprende directamente (concepto de axioma clásico);

[1] Parafraseando la famosa cita atribuida a A. Rényi (1921–1970): "Un matemático es una máquina que transforma café en teoremas."

(ii) una ley natural general verificada repetidamente (concepto de axioma de las ciencias naturales);
(iii) una afirmación fundamental en el orden lógico que no es susceptible de ser derivada de ninguna otra (concepto de axioma moderno).

En la lógica aristotélica se presentan como ejemplos de axiomas:

(a) El principio de identidad, que dice que un ente A es idéntico a un ente B si y sólo si no hay diferencia alguna entre ellos.
(b) El principio de no contradicción, que dice que nada puede ser y no ser al mismo tiempo y bajo el mismo aspecto.
(c) El principio del tercio excluso, o *Principium exclusi tertii*,[2] también *Tertium non datur* (i.e., no se da un tercero), que afirma que una proposición es o bien verdadera o bien falsa.

Hay otros muchos ejemplos. Dentro del ámbito matemático podemos mencionar:

(d) El axioma de las paralelas: Para cada recta y cada punto que no pertenece a ella existe una paralela a la misma por el mencionado punto.[3]
(e) Los axiomas de G. PEANO (1858–1932) definitorios de los números naturales, como "Todo número natural n posee exactamente un sucesor $n+1$."

Variables proposicionales y conectores lógicos. Distintas proposiciones simples pueden formar nuevas proposiciones compuestas. Por ejemplo, la proposición "Sònia está en su despacho" se puede negar: "Sònia no está en su despacho". De las proposiciones simples

"David está enfermo" y "David está en el hospital"

se puede formar

David está enfermo, por lo que está en el hospital.
David no está enfermo, pero está en el hospital.
David no está en el hospital, aunque está enfermo.

De esta manera se han unido (conectado) lógicamente dos proposiciones en principio sin relación. Tal proceso se logra usando *conectores* lógicos. Es tarea de la lógica proposicional investigar el valor de verdad o falsedad de las proposiciones compuestas a partir de los posibles valores de verdad o falsedad de sus proposiciones simples constituyentes, pero *no* los valores de verdad o falsedad de tales proposiciones simples.

El valor de verdad de las proposiciones compuestas se deduce solamente de los valores de verdad de las proposiciones simples implicadas. En nuestra lógica toda

[2] *Principium exclusii tertii sive medii inter duo contradictoria*.
[3] El axioma de las paralelas es un postulado controvertido de la geometría euclídea, con mucha historia por detrás. Vale la pena leer algo sobre el particular.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

proposición admite uno y solamente uno de los valores de verdad “verdadero” (que denotaremos por “v”) y “falso” (que denotaremos por “f”).

El lenguaje cotidiano admite muy diversas expresiones para un mismo significado, como en las tres proposiciones siguientes:

Me he hecho daño, por eso no puedo jugar.
Como me he hecho daño no puedo jugar.
Al haberme hecho daño no puedo jugar.

Esa situación no es deseable, y se puede evitar introduciendo “variables proposicionales” para las proposiciones simples, típicamente denotadas por

$$p, q, r, s \dots$$

y ciertos símbolos para los conectores lógicos. Cuatro son los conectores lógicos básicos: la negación, la conjunción, la disyunción (inclusiva), y el condicional (aunque esta se puede reducir a negación y disyunción). Existen otros dos que son muy útiles: la disyunción exclusiva u “o exclusivo”, y el bicondicional.

Negación: Dada una proposición p, la proposición $\neg p$ significa que p no es verdad y se llama la negación de p. Es verdadera si y solamente si p es falsa (y viceversa). La siguiente tabla refleja todos estos posibles valores de verdad:

p	**¬p**
v	**f**
f	**v**

Una tabla así recibe el nombre de *tabla de verdad* del conector (en este caso, de la negación). De idéntico modo se puede, pues, construir una tabla de verdad para el resto de conectores y en general para cualquier proposición compuesta.

Conjunción: Dadas dos proposiciones p y q, de denota por $p \wedge q$ a la proposición que es verdadera si sus dos proposiciones simples constituyentes son verdaderas, y falsa en otro caso:

p	**q**	**p ∧ q**
v	v	**v**
v	f	**f**
f	v	**f**
f	f	**f**

Disyunción: Dadas dos proposiciones p y q, se denota por $p \vee q$ a la proposición[4] que es verdadera siempre que por lo menos una de sus proposiciones simples constituyentes lo sea:

[4]El símbolo $\vee$ empleado para este o-inclusivo nos recuerda a la letra “v”, no sin justificación: nos remite al vocablo latino *vel*, que significa precisamente “o”.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

p	**q**	$\mathbf{p \vee q}$
v	v	**v**
v	f	**v**
f	v	**v**
f	f	**f**

Una variante de la disyunción es el "o-exclusivo", denotado por $p \veebar q$, en el que una y solamente una[5] de las proposiciones simples constituyentes es verdadera (se puede expresar también como $(p \wedge \neg q) \vee (\neg p \wedge q)$ sin necesidad de recurrir a un nuevo símbolo $\veebar$):

p	**q**	$\mathbf{p \veebar q}$
v	v	**f**
v	f	**v**
f	v	**v**
f	f	**f**

Condicional: Dadas dos proposiciones p y q, se define la proposición $p \rightarrow q$, y se llama el conector condicional de p a q, como la proposición que es falsa si p es verdadera y q es falsa, y verdadera en otro caso:

p	**q**	$\mathbf{p \rightarrow q}$
v	v	**v**
v	f	**f**
f	v	**v**
f	f	**v**

Por tanto, "$p \rightarrow q$" se toma como sinónimo de "no es el caso de que p es verdadera y q es falsa", o bien "o p es falsa o p y q son ambas verdaderas" o, lo que es lo mismo, "p es falsa o q es verdadera" (es decir, $\neg p \vee q$).

Este conector se expresa de muchas maneras: "si p es verdad, también lo es q", "q en caso de que p", "bajo la condición p se tiene q", "p es una condición suficiente para q", "q es una condición necesaria para p", entre otras.

Cuando $p \rightarrow q$ es una tautología, entonces el condicional se denomina "implicación"; se escribe $p \Rightarrow q$ y se lee "p implica q". (A veces esta lectura se hace sobre el propio condicional, por abuso del lenguaje.)

[5]Tales distinciones son a veces muy importantes, recuérdese el viejo chiste: Un matemático llega a casa, regala a su esposa un gran ramo de rosas y le dice "¡Te quiero!". Ella coge el ramo, se lo lanza a la cabeza, le da un pisotón y lo echa de casa. ¿Qué hizo mal el pobre marido? Es obvio, tendría que haber dicho: "Te quiero a ti y solamente a ti".

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

En un condicional $p \to q$, la proposición p se llama *hipótesis* o *antecedente*, y la proposición q se llama *conclusión* o *consecuente*.

El caso en que se dan simultáneamente los condicionales $p \to q$ y $q \to p$ es reseñable: se habla de un nuevo conector llamado **bicondicional**, que se denota $p \leftrightarrow q$:

$\mathbf{p}$	$\mathbf{q}$	$\mathbf{p \leftrightarrow q}$
v	v	**v**
v	f	**f**
f	v	**f**
f	f	**v**

Un bicondicional que es siempre verdadero se denomina "doble implicación", y se denota por $\Longleftrightarrow$.

Tautologías y contradicciones. Existen proposiciones cuyo valor de verdad siempre es "v": se llaman *tautologías* (del griego *tautos* = 'lo mismo'). Los axiomas son —cómo no— un ejemplo de tautologías; así, en la tabla de verdad del principio de identidad

$\mathbf{p}$	$\mathbf{p \to p}$
v	**v**
f	**v**

el valor resultante siempre es "v". Lo mismo sucede con el principio de no contradicción $\neg(p \wedge \neg p)$ y el de tercio excluso $p \vee \neg p$:

$\mathbf{p}$	$\mathbf{\neg p}$	$\mathbf{p \wedge \neg p}$	$\mathbf{\neg(p \wedge \neg p)}$	$\mathbf{p \vee \neg p}$
v	f	f	**v**	**v**
f	v	f	**v**	**v**

Las proposiciones que al ser unidas mediante el conector "$\leftrightarrow$" resultan tautologías se llaman *lógicamente equivalentes*; a veces se emplea el símbolo "$\equiv$". Por ejemplo, se tiene que $\neg(p \leftrightarrow q) \equiv p \veebar q$, o también $p \to q \equiv \neg p \vee q$.

Existen también proposiciones que resultan siempre ser falsas (todos los posibles valores de la tabla de verdad son "f"); reciben el nombre de proposiciones contradictorias o *contradicciones*. En particular, la negación de una tautología es una contradicción. Obviamente, las proposiciones que no son contradictorias siempre han de tener como mínimo un valor de verdad "v"; tales proposiciones reciben el nombre de *contingentes*.

He aquí un ejemplo de proposición contradictoria:

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

$\mathbf{p}$	$\mathbf{q}$	$\neg\mathbf{p}$	$\mathbf{p}\to\mathbf{q}$	$(\mathbf{p}\to\mathbf{q})\to\mathbf{p}$	$((\mathbf{p}\to\mathbf{q})\to\mathbf{p})\leftrightarrow\neg\mathbf{p}$
v	v	f	v	v	**f**
v	f	f	f	v	**f**
f	v	v	v	f	**f**
f	f	v	v	f	**f**

Argumentos. Un *argumento* es una aseveración de un conjunto de proposiciones $p_1, p_2, \ldots, p_n$, llamadas *premisas*, y que llevan a otra q llamada *conclusión*; es decir, se trata del condicional

$$p_1 \wedge p_2 \wedge \ldots \wedge p_n \to q.$$

Un argumento $p_1 \wedge p_2 \wedge \ldots \wedge p_n \to q$ se llama *válido* si se da la implicación

$$p_1 \wedge p_2 \wedge \ldots \wedge p_n \Longrightarrow q,$$

es decir, si el condicional es una tautología; de lo contrario se llama *falacia*. Por ejemplo, se comprueba fácilmente mediante una tabla de verdad que, dadas las proposiciones p, q, r, el argumento

$$(p \to q) \wedge (q \to r) \to (p \to r)$$

es válido.

Nota sobre el uso de paréntesis. En el caso de la aritmética usual, el resultado de $3 \cdot 4 + 5$ es 17 porque se sobreentiende que se calcula $(3 \cdot 4) + 5$; en efecto, los paréntesis son innecesarios porque se ha convenido previamente que la multiplicación es una ligadura más fuerte que la suma.

En el caso de los conectores lógicos se hace un convenio similar: la negación es el conector que liga de manera más fuerte, seguido por la conjunción $\wedge$, la disyunción $\vee$, la implicación $\to$ y la doble implicación $\leftrightarrow$ en último lugar. Así, por ejemplo, las dos proposiciones siguientes son en realidad la misma:

$$(p \vee (p \wedge q)) \to ((\neg p) \wedge (\neg q)) \vee (p \wedge q)$$

$$p \vee p \wedge q \to \neg p \wedge \neg q \vee p \wedge q$$

A menudo, por claridad y para evitar equívocos, se opta por soluciones intermedias, del estilo de

$$p \vee (p \wedge q) \to (\neg p \wedge \neg q) \vee (p \wedge q)$$

para el ejemplo anterior, en la que sólo se han omitido los paréntesis relativos a la negación y a la implicación.

—∗—

ISBN: 978-84-17900-65-6

DOI: http://dx.doi.org/10.6035/Sapientia170

Reglas de inferencia. Es muy importante en matemáticas (y en la vida) saber determinar cuándo un argumento es válido. Las consideraciones previas permiten hacerlo mediante el uso de tablas de verdad; sin embargo, existen unas reglas básicas, conocidas desde antiguo, que también pueden resultar útiles: son las llamadas reglas de inferencia. Existen cinco clásicas (cuya demostración es un mero ejercicio):

◇ *Modus ponendo ponens* (es decir, el modo que al afirmar, afirma):

$$(p \to q) \wedge p \Longrightarrow q.$$

Ejemplo: Si estás en casa te recojo; estás en casa, por tanto, te recojo.

◇ *Modus tollendo tollens* (el modo que al negar, niega)

$$(p \to q) \wedge \neg q \Longrightarrow \neg p.$$

Por ejemplo: Si llueve entonces uso el paraguas; no uso el paraguas, luego no llueve.

◇ *Silogismo hipotético*:

$$(p \to q) \wedge (q \to r) \Longrightarrow (p \to r).$$

Por ejemplo: Si te miro, te veo; si te veo, te reconozco; luego si te miro te reconozco.

◇ *Modus tollendo ponens* (el modo que al negar, afirma):

$$(p \vee q) \wedge \neg p \Longrightarrow q.$$

Por ejemplo: Es negro o blanco; no es blanco, luego es negro.

◇ *Modus ponendo tollens* (el modo que al afirmar, niega):

$$\neg(p \wedge q) \wedge p \Longrightarrow \neg q.$$

Por ejemplo: No puede ser que llueva y la plaza esté seca; llueve, luego la plaza no está seca.

Otras reglas son:

◇ *Doble negación*: $\neg\neg p \Longleftrightarrow p$
◇ *Contraposición*: $(p \to q) \Longrightarrow (\neg q \to \neg p)$
◇ *Ampliación disyuntiva*: $p \Longrightarrow p \vee q$
◇ *Simplificación disyuntiva*: $p \wedge q \Longrightarrow p$
◇ *Regla condicional*: $q \Longrightarrow (p \to q)$
◇ *Silogismo disyuntivo*: $\Big((p \vee q) \wedge (p \to r) \wedge (q \to s)\Big) \Longrightarrow (r \vee s)$
◇ *Substitución I*: $\Big((p \wedge q) \wedge (q \leftrightarrow r)\Big) \Longrightarrow (p \wedge r)$
◇ *Substitución II*: $\Big((p \to q) \wedge (p \leftrightarrow r)\Big) \Longrightarrow (r \to q)$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Predicados y cuantificadores. Las proposiciones contienen atributos que intervienen decisivamente en la manera lógica de ver y entender la realidad: los llamados *predicados*. Un predicado P es una propiedad que un sujeto puede poseer o no, pero no constituye en sí misma una proposición, aunque permite construir proposiciones, básicamente de dos formas que se complementan:

(a) Por asignación: dada una colección de objetos que tienen una cierta propiedad P, para un objeto concreto x de la colección se forma la proposición

$$P(x)$$

que quiere decir que el objeto x posee la propiedad característica de los objetos en P (con independiencia de ser esta cierta o no). Esta asignación se puede representar alternativamente por $x \in P$.

(b) Por cuantificación: dada la colección anterior, se forma una proposición que indica "cuántos" objetos de P poseen la propiedad característica de los objetos en P:

- si *todos* los objetos de la colección poseen la propiedad P se forma la proposición

$$\forall x P(x) \quad [\text{también } \forall x : P(x)].$$

El símbolo $\forall$ se lee "para todo(s)" y se llama *cuantificador universal*.

- si *al menos* un objeto de la colección posee la propiedad P, se forma la proposición

$$\exists x P(x) \quad [\text{también } \exists x : P(x)].$$

El símbolo $\exists$ es una abreviatura de "existe por lo menos un(a)"; se llama *cuantificador existencial*.

Ejemplo. Consideremos la proposición

"Los elfos blancos son más bellos que mirar al sol."[6]

En matemáticas, esta frase no se interpreta como que "por regla general", "casi siempre" son los elfos blancos más bellos que mirar al sol, sino más bien significa que "todos y cada uno", "absolutamente todos" los elfos blancos son más bellos que mirar al sol; porque en matemáticas se está interesado en proposiciones universales (que podrán tener, naturalmente, excepciones, que habrá que especificar).

En este ejemplo se distinguen dos predicados:

[6]Variación hilarante de la descripción que se da de los elfos de la luz ("Die Lichtalben sind an Gestalt schöner als die Sonne") en la adaptación al alemán moderno de la "Edda de Snorri Sturluson", conocida obra de la mitología islandesa. Cf. *Gylfis Täuschung* 17, dentro de "Die Edda des Snorri Sturluson". Adaptación de Arnulf Krause, editorial Reclam (1997).

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

P_1: ser un elfo blanco;
P_2: ser más bello que mirar al sol.

Por tanto, la proposición de partida se puede formalizar como

$$\forall x(P_1(x) \to P_2(x)).$$

Se quiere decir con ello que para todos los objetos de la clase, sin excepción, cuando se considera un elfo blanco x, es decir, $P_1(x)$, entonces x es más bello que mirar al sol, es decir, $P_2(x)$.

Para cada x lo que se encuentra entre los paréntesis externos es una proposición en forma de implicación, que asegura que cuando el antecedente es verdadero, entonces también tiene que serlo el consecuente.

Ejemplo. Consideremos la proposición

"Me como una escoba".

En principio, puede querer decir tanto que "me como exactamente una escoba", como que "me como por lo menos una". El significado del artículo indeterminado "una" no es único (¡en frases del estilo de "un país necesita paz", con "un" lo que se quiere decir es en realidad "todos"!)

En matemáticas significa "por lo menos un(a)". Para formalizar la proposición dada usando cuantificadores, se puede reformular ligeramente como

"Hay una escoba que me como".

Usando variables proposicionales y cuantificadores, se puede escribir entonces

$$\exists x(E(x) \wedge C(x)), \text{ o lo que es lo mismo, } \exists x(C(x) \wedge E(x)),$$

donde E denota el predicado "ser escoba" y C el predicado "ser comido". Entonces, $E(x)$ significa que el objeto x es una escoba, y $C(x)$ que me como x.

Los cuantificadores universal y existencial están íntimamente relacionados a través de la negación, de manera que

$$\neg(\forall x P(x)) \text{ es equivalente a } \exists x(\neg P(x))$$

y

$$\neg(\exists x P(x)) \text{ es equivalente a } \forall x(\neg P(x))$$

y

$$\forall x P(x) \text{ es equivalente a } \neg(\exists x(\neg P(x)))$$

y por último

$$\exists x P(x) \text{ es equivalente a } \neg(\forall x(\neg P(x))).$$

Un ejemplo sencillo: Las proposiciones "existe una lombriz de 150 metros" y "toda lombriz no tiene 150 metros" son negaciones mutuas.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

La noción de contraejemplo. Así, probar que una proposición $\forall x P(x)$ es falsa es lo mismo que probar que la proposición $\exists x(\neg P(x))$ es verdadera; es decir, se trata de probar la existencia de un elemento x_0 tal que $P(x_0)$ es una proposición falsa. Este elemento x_0 se llama *contraejemplo* de la proposición $\forall x P(x)$.

Ejemplo. Sea la proposición

"todo número real x verifica que $x^2 < 0$";

el número real $x_0 = 1$ es un contraejemplo a tal afirmación, pues obviamente 1 no es menor que 0, lo que prueba la falsedad del aserto. (¡De hecho, cualquier número real es un contraejemplo en este caso!)

Junto a predicados que son asignados a un solo objeto, como $P(x)$, existen también predicados de la forma

$$P(x,y), \text{ ó } Q(x,y,z), \text{ etc.,}$$

que expresan una relación entre varios objetos, como por ejemplo "ser pariente de", "ser mayor que", "ser padres de", etc. De esta forma se puede cuantificar las diferentes variables que aparecen, obteniendo expresiones del tipo

$$\forall x(\exists y P(x,y)), \;\; \exists x(\forall y P(x,y)), \;\; \forall x(\exists y(\forall z Q(x,y,z))), \quad \text{etc.}$$

(A veces se omiten los paréntesis entre cuantificadores). Aquí solamente se pueden usar nombres de variables (las letras $x,y,z,\ldots$) que no hayan sido ya empleadas en el contexto. Proposiciones del estilo

$$\forall x(\forall x P(x,x))$$

carecen de sentido. A cada variable ha de aplicarse a lo sumo un cuantificador. Se han de tener además en cuenta las reglas siguientes:

- En vez de $\forall x \forall y \forall z Q(x,y,z)$ a veces escribiremos $\forall x,y,z Q(x,y,z)$.
- La notación de las variables en una proposición cuantificada es irrelevante; por ejemplo, es lo mismo escribir $\forall \alpha P(\alpha)$ que $\forall \beta P(\beta)$. Los usos y costumbres determinan muchas veces la elección del nombre.

Una última observación: El uso de cuantificadores y conectores lógicos al mismo tiempo siempre exige precaución. Por ejemplo, $\forall x(P(x) \vee Q(x))$ no es equivalente a $(\forall x P(x)) \vee (\forall x Q(x))$. Tampoco es cierto que los operadores existencial y universal conmuten: si por ejemplo se tiene la proposición $x + y = 1$ para x e y números reales, no es cierto que sean equivalentes

$$\forall x \exists y (x + y = 1) \qquad \exists x \forall y (x + y = 1);$$

La primera es una proposición verdadera, mientras que la segunda es falsa (¿por qué?).

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

[Big] Biggs, N.L.: Discrete Mathematics. Second ed. Oxford U.P., 2004
[Bord] Bordes Solanas, M.: Las trampas de circe: falacias lógicas y argumentación informal. Cátedra, 2016
[Carr] Carroll, L.: El juego de la lógica. Alianza, 2015
[Conr] Conradie, W., Goranko, V.: Logic and Discrete Mathematics. A concise introduction. Wiley, 2015
[Dox] Doxiadis, A, Papadimitriou, Ch.: Logicomix. An epic search for truth. Bloomsbury, 2009
[Farr] Farré, R. et al.: Lógica para informáticos. Marcombo, 2011
[GOV] Galindo Pastor, C., Orús Báguena, M.P., Vindel Cañas, M.P.: Problemes de matemàtica discreta. Universitat Jaume I, 1997
[Gall] Gallier, J.: Discrete Mathematics. Springer, 2011
[Galli] Gallinari, A.: Apuntes y problemas de lógica matemática. Universidad Rey Juan Carlos, 2009
[Hasenj] Hasenjaeger, G.: Conceptos y problemas de la lógica moderna. Labor, 1968
[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3. ed. McGraw Hill, 2007
[Pla] Pla i Carrera, J.: Introducció a la metodologia de la Matemàtica. Universitat de Barcelona, 2006
[Quine1] Quine, W.V.: Selected logic papers. Random House, 1966
[Quine2] Quine, W.V.: Methods of logic. Routledge and Kegan Paul, 1966
[Rios] Ríos, S.: Matemática finita. Paraninfo, 1974
[Smull] Smullyan, R.M.: A Beginner's guide to Mathematical Logic. Dover, 2014
[Wall2] Wallis, W.D.: A beginner's guide to discrete mathematics. Second edition. Birkhäuser 2012

La referencia [**Bord**] es una buena lectura para detectar de qué manera la argumentación en el discurso actual está llena de falacias, aunque se escribe desde un punto de vista más humanístico que lógico-formal. El comic [**Dox**] es una famosa recreación de la vida y obra de Bertrand Russell, traducido a muchos idiomas. Los libros [**Quine1**] y [**Quine2**] son obras clásicas del lógico W.V. Quine cuya lectura permitiría observar hasta qué punto el lenguaje de la lógica formal no pasa de moda.

Capítulo 2. Métodos de demostración. El principio de inducción

Una mente brillante se ha dado cuenta de que

- al elevar 1 al cuadrado se obtiene de nuevo 1;
- al elevar 3 al cuadrado se obtiene 9;
- al elevar 5 al cuadrado se obtiene 25;
- al elevar 7 al cuadrado se obtiene 49.

De momento, lo único que se puede afirmar es: si se elevan los cuatro primeros números impares al cuadrado, se obtiene de nuevo un número impar. A la vista de ello uno se pregunta: ¿Sucede siempre lo mismo? Es decir, ¿siempre que se eleva un número impar al cuadrado se obtiene un número impar? O de modo más matemático: Dado un número impar n arbitrario, ¿es su cuadrado n^2 un número impar?

Si el conjunto de los números naturales $\mathbb{N}$ fuera finito, en particular lo sería el conjunto de los números impares y se podría comprobar uno por uno todos los casos y ver si el cuadrado de cada uno es otra vez impar. Pero no es el caso. ¿Cómo se puede entonces comprobar que tal afirmación es *cierta* en *todos* los casos, sin excepción? Hay que encontrar una *demostración* de ello.

Una *demostración* o *prueba* es en matemáticas una deducción reconocida como libre de fallos que comprueba la verdad o falsedad de una proposición a partir de un conjunto de axiomas, que se suponen como ciertos, y otras proposiciones ya demostradas.

Pruebas directas e indirectas. Una demostración puede ser directa o indirecta. En una *prueba directa* se demuestra la afirmación aplicando proposiciones ya probadas y concatenando una serie de conclusiones lógicas, en la que cada paso ha de ser verificado.

En una *demostración indirecta* (también llamada demostración *por reducción al absurdo* o *por contradicción*) se desea encontrar una contradicción a partir de la negación de la afirmación que se quiere demostrar. Si se llega a contradicción, no puede ser falsa la afirmación de partida y, como estamos en una lógica en las que las proposiciones son o bien verdaderas o bien falsas, ha de ser verdadera. Se basa en la regla de inferencia *Modus tollendo tollens*.

Ejemplo. Se quiere demostrar: *El cuadrado de un número natural impar n es impar.*

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Prueba directa. Sea n un número natural impar. Tal n se escribe como $n = 2k+1$, con k un número natural. Se sigue que

$$n^2 = n \cdot n = (2k+1) \cdot (2k+1) = 4k^2 + 4k + 1 = 2 \cdot (2k^2 + 2k) + 1,$$

es decir, n^2 es de la forma "2 veces un número natural + 1", o sea, n^2 es impar. □

Prueba indirecta. Supongamos que existiera un número impar m, digamos $m = 2m' + 1$ con m' un número natural, tal que m^2 no fuera impar, es decir, fuera par. Tendríamos entonces que

$$m^2 = (2m'+1)^2 = 4(m')^2 + 4m' + 1 = 4((m')^2 + m') + 1.$$

Por un lado, hemos supuesto que m^2 es par. Por otro lado, las igualdades anteriores nos muestran que m^2 es de la forma $2(2(m')^2 + 2m') + 1$, es decir, que m^2 es impar. He aquí la contradicción: un número natural puede ser o bien par o bien impar, pero no las dos cosas a la vez. □

Demos otro ejemplo de prueba por reducción al absurdo: la famosa demostración de la existencia de infinitos números primos[1] debida a Euclides:

Ejemplo (Prueba indirecta)**.** Se quiere demostrar: *Dada una cantidad finita de números primos, siempre se puede encontrar uno más (distinto).*

Demostración. Supongamos que existiera un número finito de números primos $p_1, \ldots, p_n$.

Sea $m := p_1 \cdots p_n$ el producto de todos esos primos, y consideremos el número $m+1$. Se distinguen dos casos (y solamente estos dos, luego una vez examinados habremos terminado):

(1) Si $m+1$ es un número primo, es por construcción mayor que $p_1, \ldots, p_n$ y así un primo distinto de los dados, ¡contradicción!

(2) Si $m+1$ no es primo, posee un factor primo q. Si q fuera uno de los primos $p_1, \ldots, p_n$, entonces sería un factor tanto de m como de $m+1$, y por tanto, de la diferencia $(m+1) - m = 1$, ¡absurdo!, pues q habría de ser entonces 1 y el número 1 no es primo. Entonces q ha de ser un número primo distinto de $p_1, \ldots, p_n$, lo que contradice la hipótesis de partida. □

Pruebas constructivas, casos y contraposición. Esta prueba de Euclides es realmente interesante: en primer lugar, es un buen ejemplo de demostración *no constructiva*, puesto que no nos ofrece una fórmula para el cálculo de un número primo arbitrario, sino que solamente nos muestra que uno tal debe existir. Pero también es un ejemplo de prueba por distinción de casos (casuística exhaustiva). Este es otro método de demostración.

En la *casuística exhaustiva* se quiere demostrar q, y de hecho se prueba q por un lado (caso 1) bajo la hipótesis adicional p, y por otro lado (caso 2) bajo la

[1]Un número primo es un número natural distinto de 0 y 1 que sólo es divisible por 1 y por sí mismo.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

hipótesis adicional $\neg p$. Se han de hacer cosas dos veces, pero la ventaja reside en que las hipótesis adicionales pueden conllevar métodos y técnicas que faciliten el problema inicial. Como principio de demostración posee la tabla de verdad siguiente (¡se trata evidentemente de una tautología!):

$\mathbf{p}$	$\mathbf{q}$	$\neg\mathbf{p}$	$\mathbf{p}\to\mathbf{q}$	$\neg\mathbf{p}\to\mathbf{q}$	$(\mathbf{p}\to\mathbf{q})\wedge(\neg\mathbf{p}\to\mathbf{q})$	$((\mathbf{p}\to\mathbf{q})\wedge(\neg\mathbf{p}\to\mathbf{q}))\to\mathbf{q}$
v	v	f	v	v	v	**v**
v	f	f	f	v	f	**v**
f	v	v	v	v	v	**v**
f	f	v	v	f	f	**v**

Una regla de inferencia (ya mencionada en el Capítulo 1) muy utilizada es la *contraposición*: En una demostración se toma un punto de vista pragmático, y a veces es más sencillo demostrar el condicional "$\neg q \to \neg p$" que "$p \to q$". Ambos métodos son equivalentes:

$\mathbf{p}$	$\mathbf{q}$	$\neg\mathbf{q}$	$\neg\mathbf{p}$	$\mathbf{p}\to\mathbf{q}$	$\neg\mathbf{q}\to\neg\mathbf{p}$	$(\mathbf{p}\to\mathbf{q})\leftrightarrow(\neg\mathbf{q}\to\neg\mathbf{p})$
v	v	f	f	v	v	**v**
v	f	v	f	f	f	**v**
f	v	f	v	v	v	**v**
f	f	v	v	v	v	**v**

Se distingue también entre pruebas constructivas y no constructivas, como ya indicamos tras la prueba de la existencia de infinitos números primos de Euclides. A veces se puede solamente demostrar la existencia de un objeto matemático, sin mostrar el objeto mismo. En tal caso estamos ante una demostración *no constructiva* o puramente existencial. Pero otras veces se puede dar una descripción precisa del objeto cuya existencia se quiere probar, incluso por medio de un algoritmo que calcule el objeto en cuestión: se trata de una demostración *constructiva*.

Ejemplo. Se quiere demostrar: *La función real de variable real* $f(x) = 2x - 1$ *posee un cero* x_0 *tal que* $0 \leq x_0 \leq 1$.

Demostración constructiva. Sea $x_0 = \frac{1}{2}$. Entonces

$$f(x_0) = 2 \cdot x_0 - 1 = 2 \cdot \frac{1}{2} - 1 = 1 - 1 = 0,$$

esto es, $x_0 = \frac{1}{2}$ es un cero de f. Obviamente se cumple que $0 \leq \frac{1}{2} \leq 1$, lo que prueba la afirmación inicial. □

En esta demostración se observa no solamente que existe un cero, sino también cuál es: $x_0 = \frac{1}{2}$. Se ha intuido de alguna manera cuál era la solución. Adivinar posibles soluciones es una propiedad que se puede entrenar, pero al mismo tiempo hace de la Matemática —sobre todo al principio— una disciplina no muy agradecida.

Demostración existencial o no constructiva. La función f es continua en todo $\mathbb{R}$, en particular entre 0 y 1 (incluyendo los mismos 0 y 1). Además verifica que $f(0) = -1 < 0$ y $f(1) = 1 > 0$. Por tanto, estamos en condiciones de aplicar un corolario del teorema de Bolzano.[2] □

¡Sobre el valor del cero en cuestión esta última prueba no dice nada!

Un método de demostración muy importante es el *principio de inducción*. Con él se pueden demostrar enunciados que afectan a números naturales. Posee una estructura que se basa en la axiomática de los números naturales (axiomas de Peano), como veremos en el capítulo 12.

Sea A una afirmación sobre números naturales.

(AI) *Apertura inductiva*: (Se demuestra:) A es cierta para el natural n_0.
(HI) *Hipótesis de inducción* (Se supone:) A es cierta para *un* natural $n \geq n_0$.
(PI) *Paso inductivo*: (Se demuestra:) De la (HI) se sigue que A también es cierta para $n+1$.
(CI) *Conclusión inductiva*: (Se colige:) Por ello A es válida para todos los números naturales $\geq n_0$.

Ejemplo. Para todo número natural $n \geq 1$ se tiene que

$$1+2+3+4+\cdots+n = \frac{n(n+1)}{2}.$$

Lo demostraremos por medio del principio de inducción.

(AI) La afirmación es correcta para el número natural $n_0 = 1$, puesto que $1 = \frac{1(1+1)}{2}$.
(HI) Supongamos que la afirmación fuera correcta para un número natural $n \geq n_0 = 1$.
(PI) Se cumple que

$$\begin{aligned} 1+\cdots+n+(n+1) &= (1+\cdots+n)+(n+1) = \frac{n(n+1)}{2}+n+1 \\ &= \frac{n(n+1)+2(n+1)}{2} = \frac{(n+1)(n+2)}{2}. \end{aligned}$$

Nótese que en la segunda igualdad se ha aplicado (HI).
(CI) La afirmación se verifica para todo número natural $n \geq 1$.

El esquema de inducción describe una propiedad fundamental de los números naturales, que en última instancia no se puede deducir de propiedades más sencillas de tales números. Precisa el argumento "... y así sucesivamente". La denominación

[2] Esta consecuencia del teorema debido a B. BOLZANO (1781–1848) afirma: Sea I un intervalo abierto, sea $f : I \to \mathbb{R}$ una función continua en I con $a, b \in I$ y $a \leq b$. Supongamos que para un $c \in \mathbb{R}$ se tiene $f(a) \leq c \leq f(b)$ (o $f(b) \leq c \leq f(a)$). Entonces existe un ξ tal que $a \leq \xi \leq b$ con $f(\xi) = c$.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

y estructura de las partes del esquema puede variar según autores; normalmente se consideran solamente los pasos (AI), (HI) y (PI).

Con el principio de inducción están muy relacionadas las definiciones recursivas. Por el momento solamente mencionaremos algunos ejemplos muy útiles. En primer lugar, ya hemos empleado sumas del tipo

$$1+\cdots+n$$

de forma no muy satisfactoria, pues la notación "$\cdots$" no es en absoluto precisa, a priori.[3] Como primer ejemplo de definición recursiva introducimos el símbolo de la suma o *sumatorio*:

$$\sum_{k=0}^{0} a_k := a_0,$$
$$\sum_{k=0}^{n} a_k := \sum_{k=0}^{n-1} a_k + a_n \quad \text{para } n \geq 1.$$

Ciertamente de forma poco precisa retornaremos ocasionalmente a la notación anterior, es decir, para $m \leq n$ escribiremos

$$\sum_{k=m}^{n} a_k = a_m + \cdots + a_n.$$

Por motivos prácticos se define $\sum_{k=m}^{n} a_k := 0$ para $n < m$, y se habla entonces de la *suma vacía*.

Ahora ya podemos dotar de sentido a la expresión $1+\cdots+n$. Se define como el sumatorio

$$1+\cdots+n := \sum_{k=1}^{n} k.$$

Demos una generalización inmediata del símbolo de la suma: Para cualesquiera dos números enteros m,n tales que $m \leq n$, sea

$$\sum_{k=m}^{n} a_k := \sum_{k=0}^{n-m} a_{k+m}$$

(esta definición permite mover el contador de la suma arbitrariamente). Las reglas siguientes (fácilmente demostrables) las usaremos una y otra vez:

$$\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n} (a_k + b_k), \qquad c \cdot \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} c a_k.$$

[3] Es pertinente citar aquí el comentario que cierto catedrático le escribió al autor de estas líneas en su época de estudiante cuando dio por demostrados unos puntos suspensivos: "No dejes que la intuición substituya a la inducción".

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Análogamente se introduce el símbolo $\prod$ para el producto:

$$\prod_{k=0}^{0} a_k := a_0,$$
$$\prod_{k=0}^{n} a_k := \prod_{k=0}^{n-1} a_k \cdot a_n \quad \text{para } n \geq 1.$$

Otro ejemplo de definición recursiva lo constituyen las potencias de un número real a:

$$a^0 := 1, \qquad a^n := a^{n-1} \cdot a,$$

donde los exponentes n son números naturales.

Para practicar el principio de inducción demostramos ahora la siguiente fórmula, relacionada con las potencias:

Teorema 2.1. *(Suma geométrica). Sea a un número real distinto de* 1*. Se tiene que*

$$\sum_{k=0}^{n} a^k = \frac{1-a^{n+1}}{1-a}$$

para cualquier número natural n.

Demostración. Apliquemos el principio de inducción sobre n:
(AI) La afirmación es correcta para $n_0 = 0$ de manera obvia, pues

$$\sum_{k=0}^{0} a^k = a^0 = 1 = \frac{1-a^{0+1}}{1-a} = \frac{1-a}{1-a}.$$

(HI) Suponiendo que la fórmula es válida para cierto $n \geq 0$...
(PI) ... lo será también para $n+1$, pues

$$\sum_{k=0}^{n+1} a^k = \sum_{k=0}^{n} a^k + a^{n+1} \overset{(HI)}{=} \frac{1-a^{n+1}}{1-a} + a^{n+1}$$
$$= \frac{1-a^{n+1}+a^{n+1}(1-a)}{1-a} = \frac{1-a^{n+2}}{1-a}.$$

(CI) La afirmación es válida entonces para cualquier número natural. □

Sea $n \geq 1$ un número natural. Se define el *factorial de n*

$$n! := \prod_{i=1}^{n} i \quad (= 1 \cdot 2 \cdot 3 \cdots n).$$

Completamos la definición de $n!$ con

$$0! := 1.$$

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

Estrechamente vinculados a $n!$ se encuentran los *coeficientes binomiales* (o números combinatorios). Para cualesquiera números naturales n,k con $n \geq k$ se define

$$\binom{n}{k} := \frac{n!}{k!(n-k)!};$$

si $n < k$ entonces $\binom{n}{k} := 0$. El símbolo $\binom{n}{k}$ se lee "n sobre k". Para el cálculo de números combinatorios resulta muy útil el resultado siguiente, del que damos una prueba directa a partir de la definición de los números combinatorios involucrados.

Teorema 2.2. *Para cualesquiera k,n números naturales tales que $n \geq k > 0$ se verifica la igualdad*

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

Demostración. Para $k = n$ y $k = 1$ se deduce inmediatamente la fórmula. Para $1 < k < n$ se tiene:

$$\begin{aligned}\binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n+1-k)!} \\ &= \frac{n!(n-k+1)+n!(k)}{k!(n+1-k)!} = \frac{n!((n-k+1)+k)}{k!(n+1-k)!} \\ &= \frac{(n+1)!}{k!(n+1-k)!} = \binom{n+1}{k}.\end{aligned}$$ □

Los coeficientes binomiales deben su nombre al siguiente resultado:

Teorema 2.3. *(Fórmula del binomio de Newton).*[4] *Sean a,b números reales. Para todo número natural n se tiene que*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

[4] Isaac NEWTON, celebérrimo matemático inglés (1643–1727).

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Demostración. Aplicaremos el principio de inducción a n. Obviamente basta con que verifiquemos el paso inductivo (PI):

$$\begin{aligned}(a+b)^{n+1} &= (a+b)(a+b)^n = (a+b)\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k \\ &= \sum_{k=0}^{n}\binom{n}{k}a^{n+1-k}b^k + \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^{k+1} \\ &= a^{n+1} + \sum_{k=1}^{n}\binom{n}{k}a^{n+1-k}b^k + \sum_{k=0}^{n-1}\binom{n}{k}a^{n-k}b^{k+1} + b^{n+1} \\ &= a^{n+1} + \sum_{k=1}^{n}\binom{n}{k}a^{n+1-k}b^k + \sum_{k=1}^{n}\binom{n}{k-1}a^{n+1-k}b^k + b^{n+1} \\ &= a^{n+1} + \sum_{k=1}^{n}\left(\binom{n}{k} + \binom{n}{k-1}\right)a^{n+1-k}b^k + b^{n+1} \\ &= a^{n+1} + \sum_{k=1}^{n}\binom{n+1}{k}a^{n+1-k}b^k + b^{n+1} \\ &= \sum_{k=0}^{n+1}\binom{n+1}{k}a^{n+1-k}b^k.\end{aligned}$$

Para ello se ha efectuado un cambio de subíndices y se ha usado el Teorema 2.2.

□

Los coeficientes binomiales se describen fácilmente gracias al Teorema 2.2 con la ayuda del *triángulo de Pascal* (por el filósofo, físico y matemático francés Blaise PASCAL (1623–1662)):

$$\begin{array}{ccccccccccc} & & & & & 1 & & & & & \\ & & & & 1 & & 1 & & & & \\ & & & 1 & & 2 & & 1 & & & \\ & & 1 & & 3 & & 3 & & 1 & & \\ & 1 & & 4 & & 6 & & 4 & & 1 & \\ 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\ & & & & & \dots & & & & & \end{array}$$

La n-ésima fila del dibujo ($n = 0,1,2\dots$) contiene por orden los coeficientes binomiales $\binom{n}{k}$ ($k = 0,\dots,n$). Estos se obtienen, para $1 \leq k \leq n-1$, por adición de los dos situados directamente encima, reencontrando el resultado del Teorema 2.2.

En capítulos posteriores volveremos a encontraremos tanto el factorial como los coeficientes binomiales en un contexto puramente combinatorio: condensan la respuesta a ciertos problemas de conteo.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

[Cab] Caballero Roldán, Rafael et al.: Matemática Discreta para Informáticos. Ejercicios resueltos. Pearson/Prentice Hall, 2007

[Conr] Conradie, W., Goranko, V.: Logic and Discrete Mathematics. A concise introduction. Wiley, 2015

[GOV] Galindo Pastor, C., Orús Báguena, M.P., Vindel Cañas, M.P.: Problemes de matemàtica discreta. Universitat Jaume I, 1997

[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3. ed. McGraw Hill, 2007

[Pla] Pla i Carrera, J.: Introducció a la metodologia de la Matemàtica. Universitat de Barcelona, 2006

[Trias] Trias Pairó, J.: Matemàtica discreta. Problemes resolts. Universitat Politècnica de Catalunya, 2009

[Wall2] Wallis, W.D.: A beginner's guide to discrete mathematics. Second edition. Birkhäuser, 2012

Capítulo 3. Conjuntos

Una parte importante del lenguaje matemático moderno está constituida por conjuntos, aplicaciones y operaciones relacionadas con ellos. Los símbolos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ no denotan simplemente números sueltos, sino determinadas *colecciones* de números.

En este curso vamos a suponer que el lector tiene una idea intuitiva de la definición de "conjunto": no podemos dar una definición precisa del concepto "conjunto", pero esto no va a suponer ninguna obstrucción para nuestros objetivos. El creador de la teoría de conjuntos, el alemán Georg CANTOR (1845–1918), lo describió así: Un *conjunto*[1] M es una reunión en un todo de determinados objetos, claros y distintos, de nuestra experiencia o de nuestro pensamiento (que llamaremos *elementos* de M).

Los objetos que se reúnen para formar un conjunto se llaman, como escribió Cantor, *elementos* de ese conjunto.

Vocabulario básico. La pertenencia de un elemento a un conjunto se expresa con el símbolo $\in$ (queriendo abreviar "est", ser/estar en latín), y la no pertenencia por $\notin$; por ejemplo

$$\pi \in \mathbb{R}, \qquad \sqrt{2} \notin \mathbb{Q}$$

Un conjunto se representa o bien por medio de un diagrama de Venn[2], que es una elipse que encierra la colección de elementos constituyentes del conjunto, como luego veremos, o bien a través de llaves entre las que se escriben los elementos, como en

$$\{a,e,i,o,u\}, \qquad \{2,3,5,7,11,13,17,19,23\}.$$

A la reunión de ningún objeto también la consideraremos un conjunto, llamado el *conjunto vacío*; se denota por $\varnothing$, ¡y no por $\{\varnothing\}$, que tiene otro significado!

A menudo definiremos conjuntos M como una colección de elementos de otro conjunto que satisfacen una cierta propiedad; en este caso es útil la notación "dos

[1]En alemán, "conjunto" se dice "Menge". La definición original en alemán dada por Cantor, y que hemos traducido libremente en el texto, es: "Eine *Menge* M ist die Zusammenfassung von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens (welche die *Elemente* von M genannt werden) zu einem Ganzen".

[2]En honor al matemático británico John VENN (1834–1923).

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

puntos igual" que indica que se está definiendo el conjunto M, por ejemplo

$$M := \{n \in \mathbb{N} : n \text{ impar}\};$$

aquí $\{\dots\}$ es la pareja de llaves que indica que se trata de un conjunto, y definimos M (tal definición se expresa usando el símbolo $:=$) como el conjunto de todos los números naturales impares. De manera poco precisa escribiremos a veces $M := \{1,3,5,7,\dots\}$, así como $\mathbb{N} = \{0,1,2,\dots\}$ o $\mathbb{Z} = \{\dots,-2,-1,0,1,2,3,4,\dots\}$, por poner dos ejemplos.

Se pueden describir conjuntos *por extensión*, es decir, explicitando todos y cada uno de sus elementos, como en

$$\{1,2,3,4,5,6,7,8,9,10,11\},$$

o *por comprensión*, esto es, dando propiedades características de sus elementos:

$$\{n \in \mathbb{N} : 1 \leq n \leq 11\}.$$

Ocurre que a veces queremos considerar una reunión de elementos que pertenecen a un conjunto mayor, pero no tomar todos. Tal reunión forma un conjunto que llamaremos *subconjunto* del conjunto mayor. Lo denotaremos por $\subseteq$:

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}.$$

Se lee: $\mathbb{N}$ está contenido en $\mathbb{Z}$, $\mathbb{Z}$ está contenido en $\mathbb{Q}$, etc. Entonces

$$A \subseteq B \text{ se define como } \forall x(x \in A \to x \in B).$$

Es decir, un conjunto A es subconjunto de un conjunto B si todo elemento de A lo es también de B. El conjunto vacío $\varnothing$ siempre es subconjunto de cualquier conjunto. Para indicar que un conjunto no es subconjunto de otro escribiremos $A \not\subseteq B$, como en $\mathbb{Z} \not\subseteq \mathbb{N}$.

Si se quiere incidir en que todos los de B están en A pero no todos los de A están en B se dice que A es un *subconjunto propio* de B, y se escribe $\subsetneq$, como en

$$\mathbb{N} \subsetneq \mathbb{Z};$$

se lee: todo número natural es entero, pero no todo entero es natural; o bien: $\mathbb{N}$ está contenido estrictamente en $\mathbb{Z}$. Por tanto, $A \subsetneq B$ significa

$$\forall x : (x \in A \to x \in \ B) \land \exists y : (y \in B \land y \notin A).$$

Ahora bien, puede pasar que un conjunto A esté contenido en otro B y viceversa: entonces se dice que los conjuntos son iguales, y se escribe $A = B$. Es decir:

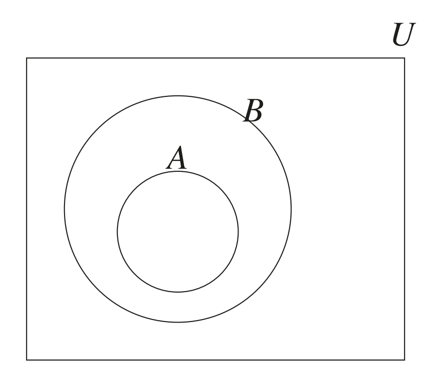
$$A = B \quad \text{ si y solamente si } \quad A \subseteq B \text{ y } B \subseteq A.$$

Esto equivale a decir: dos conjuntos son iguales si y solamente si poseen los mismos elementos.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Muchas veces se trabaja con conjuntos contenidos todos en uno mayor, que se llama *universo* y se denota por U. Si es este el caso, lo fijaremos de antemano.

Ya hemos mencionado que un método para la visualización de conjuntos son los *diagramas de Venn*, que representan un conjunto como el interior de una curva cerrada simple (una circunferencia o elipse, o similares). Por ejemplo, si A y B son conjuntos dentro de un universo U, el hecho de que A sea un subconjunto de B se representa mediante diagramas de Venn como:



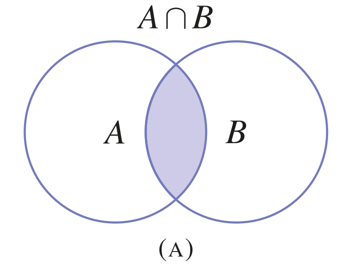
Nótese que el universo U se ha representado como un rectángulo, para resaltar su carácter especial. No es inusual obviar su representación. De ahora en adelante en este capítulo se supondrá que todos los conjuntos son subconjuntos de un conjunto universo U.

Operaciones conjuntistas. Veamos qué operaciones básicas se pueden efectuar con conjuntos. La *intersección* $A \cap B$ de dos conjuntos A, B viene dada por los elementos que pertenecen a ambos conjuntos, es decir

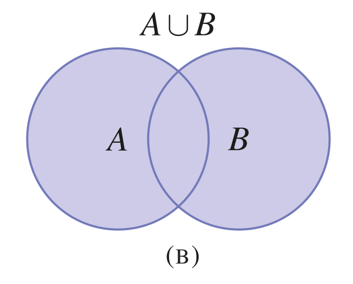
$$A \cap B = \{x \in U : x \in A \ \wedge \ x \in B\}.$$

Dos conjuntos A, B tales que $A \cap B = \varnothing$ se denominan conjuntos *disjuntos*. Su *unión* $A \cup B$ está formada por los elementos que pertenecen a uno u otro conjunto (o a ambos: aquí se usa la conjunción coordinada disyuntiva "o" en sentido inclusivo)

$$A \cup B = \{x \in U : x \in A \ \vee \ x \in B\}.$$



(A)



(B)

Ejemplo. Es muy fácil comprobar que:

$$\{1,2,3\} \cup \varnothing = \{1,2,3\},$$
$$\{1,2,3\} \cap \varnothing = \varnothing,$$
$$\{1,2,3\} \cup \{2,3,4,5\} = \{1,2,3,4,5\},$$
$$\{1,2,3\} \cap \{2,3,4,5\} = \{2,3\}.$$

Además se define el *complemento de B en A*, o *diferencia* de B y A como el conjunto de los elementos que pertenecen a A pero no a B:

$$A \setminus B = \{x \in U : x \in A \ \wedge \ x \notin B\}.$$

Si A es el conjunto universo, se escribe $U \setminus B =: \bar{B}$, y se habla simplemente del complemento de B.

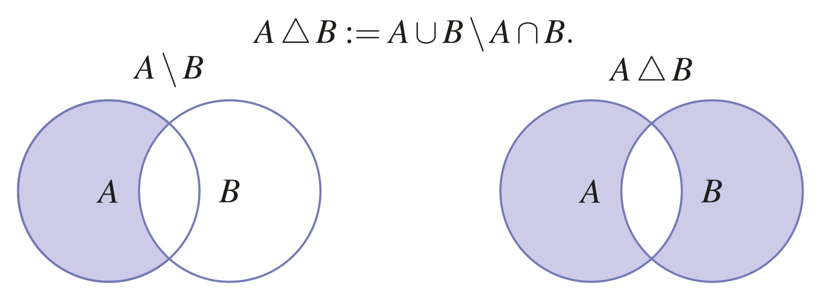
Por ejemplo, si $A = \{1,2,3\}$ y $B = \{1,2,4\}$, entonces $B \setminus A = \{4\}$ y $A \setminus B = \{3\}$. Efectivamente

$$A \setminus B \neq B \setminus A.$$

Esto no sucede con la unión y la intersección de dos conjuntos: siempre se tiene que $A \cup B = B \cup A$ y que $A \cap B = B \cap A$. Se dice que la unión y la intersección de conjuntos son *conmutativas*. La unión e intersección de conjuntos cumplen muchas propiedades de demostración inmediata, entre ellas: $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, y las análogas intercambiando $\cup$ por $\cap$.

Los elementos que están en un conjunto A o en uno B pero no en ambos forman la *diferencia simétrica* de A y B:

$$A \triangle B := A \cup B \setminus A \cap B.$$



Una característica importante de un conjunto M es su *cardinal*, denotado $|M|$ o a veces también $\#(M)$: es el número de elementos que contiene. Si M es finito, se escribe $|M| < \infty$; si sabemos que consta de n elementos, escribiremos

$$|M| = n.$$

Para conjuntos infinitos se emplea la notación

$$|M| = \infty.$$

ISBN: 978-84-17900-65-6

DOI: http://dx.doi.org/10.6035/Sapientia170

Otra construcción importante es el *producto cartesiano*[3] de dos conjuntos:

$$A \times B = \{(a,b) : a \in A, b \in B\};$$

se denota por (a,b) al *par ordenado* con primera componente a en A y segunda componente b en B. Si $a \neq b$, es obvio que

$$(a,b) \neq (b,a)$$

(por el contrario $\{a,b\} = \{b,a\}$). De acuerdo con el matemático polaco K. KURATOWSKI (1896–1980), un par ordenado (a,b) se define como el conjunto $\{\{a\},\{a,b\}\}$. Nótese que $A \times \varnothing = \varnothing \times A = \varnothing$. Si $A = B$, en lugar de $A \times A$ se suele escribir A^2 (¡Cuidado, esto no se lee "A cuadrado"!).

Ejemplos. (i) Para $A = \mathbb{R}$, el producto cartesiano $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ ya nos resulta familiar: hemos oído con seguridad más de una vez que todo punto del plano se corresponde con un par (x,y) con $x,y \in \mathbb{R}$.
(ii) Sean $A = \{1,2\}$ y $B = \{a,b,c\}$. Se tiene que

$$\begin{aligned} A \times B &= \{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c)\} \\ B \times A &= \{(a,1),(a,2),(b,1),(b,2),(c,1),(c,2)\} \end{aligned}$$

Se observa que $A \times B \neq B \times A$; efectivamente, el producto cartesiano de conjuntos no es, en general, conmutativo.

Por supuesto, intersección, unión y producto cartesiano se pueden definir para un número finito de conjuntos, no solamente para dos:

$$\begin{aligned} M_1 \cap \cdots \cap M_n &= \bigcap_{i=1}^{n} M_i = \bigcap_{i \in \{1,\ldots,n\}} M_i := \{x : x \in M_i \text{ para todo } i \in \{1,\ldots,n\}\} \\ M_1 \cup \cdots \cup M_n &= \bigcup_{i=1}^{n} M_i = \bigcup_{i \in \{1,\ldots,n\}} M_i := \{x : x \in M_i \text{ para un } i \in \{1,\ldots,n\}\} \\ M_1 \times \cdots \times M_n &:= \{(x_1,\ldots,x_n) : x_i \in M_i \text{ para } 1 \leq i \leq n\}, \end{aligned}$$

donde el conjunto $\{1,\ldots,n\}$ se llama simplemente *conjunto de subíndices*.

El producto cartesiano del conjunto M consigo mismo n-veces se denota por M^n. Esta formado por todas las n-uplas $(x_1,\ldots,x_n)$ con $x_1,x_2,\ldots,x_n \in M$:

$$M^n = \{(x_1,\ldots,x_n) : x_i \in M \text{ para todo } i = 1,\ldots,n\}.$$

Conjunto potencia. Para terminar el capítulo, consideraremos una última manera de construir nuevos conjuntos a partir de uno dado. Sea M un conjunto. El conjunto

[3] Por el filósofo y matemático francés René DESCARTES (1596–1650), que latinizó su nombre a Renatus Cartesius.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

de todos los subconjuntos de M se llama *potencia* de M (también se denomina el *conjunto de partes de M*), y se denota por $\mathscr{P}(M)$. Así pues, por definición

$$A \in \mathscr{P}(M) \Longleftrightarrow A \subseteq M.$$

Ejemplos. (i) $\mathscr{P}(\varnothing) = \{\varnothing\}$.
(ii) $\mathscr{P}(\{a\}) = \big\{\varnothing, \{a\}\big\}$.
(iii) Sea $M = \{a, b, 1\}$. Entonces el conjunto potencia de M es

$$\mathscr{P}(M) = \big\{\varnothing, \{a\}, \{b\}, \{1\}, \{a,b\}, \{a,1\}, \{b,1\}, \{a,b,1\}\big\}.$$

(iv) $\mathscr{P}(\mathscr{P}(\varnothing)) = \big\{\varnothing, \{\varnothing\}\big\}$.
(v) $\mathscr{P}(\mathscr{P}(\{a\})) = \big\{\varnothing, \{\varnothing\}, \{\{a\}\}, \{\varnothing, \{a\}\}\big\}$.

La dificultad para el principiante radica en el hecho de que los elementos del conjunto potencia son, a su vez, conjuntos. Nótese, así mismo, la diferencia de uso entre los símbolos "$\in$" y "$\subseteq$" en este contexto: se escribe

$$\{a\} \in \mathscr{P}(\{a\}), \quad \text{pero} \quad \big\{\{a\}\big\} \subseteq \mathscr{P}(\{a\}) \quad \text{y así} \quad \big\{\{a\}\big\} \in \mathscr{P}(\mathscr{P}(\{a\})).$$

En (iii) del ejemplo anterior vemos que $|M| = 3$ y que $\mathscr{P}(\{a, b, 1\})$ posee $2^3 = 8$ elementos. Este hecho es general:

Teorema 3.1. *Para un conjunto finito M con n elementos, el conjunto $\mathscr{P}(M)$ tiene cardinal 2^n, para todo $n \in \mathbb{N}$.*

Demostración. Apliquemos el principio de inducción sobre n:

(AI) Para $n = 0$ está claro, pues $M = \varnothing$ y $|\mathscr{P}(\varnothing)| = |\{\varnothing\}| = 1 = 2^0 = 2^{|\varnothing|}$.

(HI) Supongamos que para un cierto $n \geq 0$, si $|M| = n$ entonces $|\mathscr{P}(M)| = 2^n$.

(PI) Veamos ahora que para un conjunto M de $n+1$ elementos su potencia tiene cardinal 2^{n+1}. Sea para ello $M = \{a_1, \dots, a_n, a_{n+1}\}$. Dado un subconjunto S de M puede pasar:

(i) Que $a_{n+1} \notin S$, y entonces $S \subseteq \{a_1, \dots, a_n\}$ y por (HI) hay exactamente 2^n subconjuntos de M de este tipo, es decir, para $M_1 := \{S \subseteq M : a_{n+1} \notin S\}$ se tiene que $|M_1| = 2^n$.

(ii) Que $a_{n+1} \in S$, y entonces $S \setminus \{a_{n+1}\} \subseteq \{a_1, \dots, a_n\}$ y de nuevo por (HI), si $M_2 := \{S \subseteq M : a_{n+1} \in S\}$, entonces $|M_2| = 2^n$.

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

Además, estos dos casos se excluyen mutuamente y son todos los posibles, luego

$$|\mathscr{P}(M)| = |M_1| + |M_2| = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}.$$

(CI) Se deduce que para todo $n \in \mathbb{N}$, si $|M| = n$ entonces $|\mathscr{P}(M)| = 2^n$. □

Teoría axiomática de conjuntos. La teoría anterior se considera suficiente como vehículo de comunicación en matemáticas, pues es equivalente a la lógica de predicados (o de primer orden), es decir, a la lógica proposicional dotada de los cuantificadores universal y existencial. Precisamente por ello, ya el mismo Cantor y su compatriota Gottlob FREGE (1848–1925) intentaron *axiomatizar* esta teoría *naïve* de conjuntos: no se trata tanto de definir la noción de conjunto como de describir qué relaciones entre conjuntos queremos suponer para, a partir de ellas, ir construyendo todo el edificio de las matemáticas. Se parte, pues, de que hay conjuntos y de que se tiene la relación $\in$ (elemento). Frege propone un primer axioma de *extensionalidad*: Dos conjuntos son iguales si y solamente si poseen los mismos elementos; traducido a la lógica de predicados:

$$\forall X \forall Y \Big(\forall Z (Z \in X \longleftrightarrow Z \in Y) \longrightarrow X = Y \Big).$$

Formaliza la descripción de un conjunto por extensión. También lo podemos hacer por comprensión, lo que corresponde al fregeliano *axioma de comprehensión:* Para cada propiedad $\mathfrak{P}$ (de conjuntos) existe un conjunto X cuyos elementos son exactamente todos aquellos conjuntos que cumplen $\mathfrak{P}$. El conjunto que corresponde a $\mathfrak{P}$ es único (por el axioma de extensionalidad) y lo denotamos por

$$\{Z : \mathfrak{P}(Z)\}.$$

El axioma de comprehensión permite definir muchos conjuntos. Por ejemplo, para la propiedad $Z \neq Z$ se define el conjunto sin elementos (vacío) $\varnothing := \{Z : Z \neq Z\}$. Pero también conduce a arenas movedizas: el británico Bertrand RUSSELL (1872–1970) descubre en seguida[4] la inconsistencia de la teoría en este axioma, enunciando lo que se llama la *antinomia* (o paradoja) *de Russell*: se puede tomar $Z \notin Z$ como propiedad $\mathfrak{P}$, y así formar el conjunto

$$M' = \{Z : Z \notin Z\}.$$

Esto significa que para un elemento (conjunto) X cualquiera,

$$X \in M' \longleftrightarrow X \notin X;$$

pero si elegimos como X el propio conjunto M', llegamos a la contradicción

$$M' \in M' \longleftrightarrow M' \notin M'.$$

[4] Algunos autores, como Walter PURKERT, sostienen que de esto ya se habría percatado Cantor con anterioridad, cf. [**Pur**].

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

Tras el descubrimiento de esta y otras contradicciones, el propio Russell, así como Ernst ZERMELO (1871–1953) y otros se propusieron reparar la axiomática conjuntista de Frege con el fin de dejarla libre de contradicciones. Zermelo y más tarde Abraham Adolf FRAENKEL (1891–1965) y Thoralf SKOLEM (1887–1963), establecieron una axiomática considerada aún hoy libre de contradicciones. (Decimos "considerada" porque, con las herramientas de la propia teoría de conjuntos, es imposible probar si un sistema axiomático de la misma está o no libre de contradicciones, según un teorema de Kurt GÖDEL (1906–1978).)

El resultado es un sistema axiomático que conserva el espíritu de las propuestas de Cantor y Frege, pero corrige sus puntos débiles. En el caso del axioma de comprehensión, este se substituye por el *axioma de especificación:* Para cada conjunto X y cada propiedad $\mathfrak{P}$ formulable por medio de la lógica de predicados, existe un conjunto cuyos elementos son exactamente aquellos elementos $Z \in X$ para los que se cumple la propiedad $\mathfrak{P}$; ya no se puede considerar $M' = \{Z : Z \notin Z\}$ sino

$$M = \{Z \in Y : Z \notin Z\},$$

donde Y es un conjunto (de conjuntos) del que se sabe que existe. Ahora $M \in M$ es imposible (ya que si fuera posible, tendríamos $M \in Y$ y $M \notin M$, contradicción). Luego $M \notin M$, lo que implica $M \notin Y$ (pues de lo contrario, si $M \in Y$, como $M \notin M$, habría de ser $M \in M$, contradicción).

Con la consideración de M en vez de M' (es decir, con el nuevo axioma de especificación), han cambiado las cosas: si Y es un conjunto cualquiera que existe, hemos visto que el conjunto M no puede ser elemento de Y. La existencia de un conjunto Y se garantiza dentro del sistema por el *axioma de existencia*: existe al menos un conjunto. La antinomia de Russell se desvanece.

El conjunto axiomático de Zermelo-Fraenkel consta de algunos axiomas más; se suele aceptar entre ellos el llamado *axioma de elección*, que en una de sus formulaciones dice: Sea X un conjunto de conjuntos disjuntos dos a dos $Z_i \neq \varnothing$; entonces existe un conjunto que tiene exactamente un elemento en común con cada Z_i. Fue controvertido aceptarlo como axioma por motivos que no podemos explicar aquí, de hecho algunos matemáticos todavía se resisten. Lo cierto es que posibilita probar ciertos resultados útiles, muchas veces formulaciones equivalentes del propio axioma de elección, como por ejemplo que cualquier espacio vectorial (sea finito-dimensional o no) posee al menos una base.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

[Ant] Antoine, R., Camps, R., Moncasi, J.: Introducció a l'àlgebra abstracta. Universitat Autònoma de Barcelona, 2007
[Big] Biggs, N.L.: Discrete Mathematics. Second ed. Oxford U.P., 2004
[Conr] Conradie, W., Goranko, V.: Logic and Discrete Mathematics. A concise introduction. Wiley, 2015
[FG] Ferrando, J.C., Gregori, V.: Matemática Discreta. 2. ed. Reverté, 2002
[GOV] Galindo Pastor, C., Orús Báguena, M.P., Vindel Cañas, M.P.: Problemes de matemàtica discreta. Universitat Jaume I, 1997
[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3. ed. McGraw Hill, 2007
[Pla] Pla i Carrera, J.: Introducció a la metodologia de la Matemàtica. Universitat de Barcelona, 2006
[Pur] Purkert, W., Ilgauds, H.J.: Georg Cantor. Vita Mathematica, Birkhäuser 1987
[Rios] Ríos, S.: Matemática finita. Paraninfo, 1974
[Wall2] Wallis, W.D.: A beginner's guide to discrete mathematics. Second edition. Birkhäuser 2012

Capítulo 4.
Relaciones binarias

La clasificación de objetos matemáticos de acuerdo a ciertas propiedades prefijadas es una de las tareas principales de esta disciplina. Por ejemplo, los polígonos en el plano se clasifican según su número de vértices (conocemos desde el colegio la clasificación en triángulos, cuadriláteros, pentágonos, hexágonos, heptágonos, octógonos, eneágonos, decágonos, endecágonos, dodecágonos, tridecágonos, tetradecágonos...); los números naturales se clasifican en pares o impares según sean divisibles por dos o no lo sean. Y como estos, existen muchos más ejemplos. ¿Cómo dotar de una formulación matemática a este hecho?

Las relaciones binarias ofrecen un lenguaje para *comparar* dos elementos de un cierto conjunto, de foma que se dicen relacionados si tienen en común la propiedad a debate. Por ejemplo, si la propiedad fuera "tener tantos hermanos como", diríamos que dos individuos en una cierta población (el conjunto A) están relacionados (por medio de la relación mencionada) si tienen el mismo número de hermanos. Esto permitiría formar grupos en esa población en función del número de hermanos que tuvieran.

El medio matemático más eficaz para comparar dos elementos de un conjunto ya lo conocemos: Adquiere particular relevancia en este contexto el *producto cartesiano* de dos conjuntos A y B, que, como vimos en el capítulo 3, es el conjunto

$$A \times B = \{(a,b) : a \in A, b \in B\};$$

se denota por (a,b) al *par ordenado* con primera componente a y segunda componente b. Recordemos que si $a \neq b$ entonces

$$(a,b) \neq (b,a)$$

(por el contrario $\{a,b\} = \{b,a\}$). Si $A = B$, en vez de $A \times B$ se escribe también A^2. Así por ejemplo, el caso $A = \mathbb{R}$ es familiar: a todo punto del plano se asigna una pareja de números reales (las *coordenadas*) que se corresponde exactamente con un elemento de $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Los subconjuntos de un producto cartesiano de dos conjuntos son el objeto central de este capítulo:

Definición. Sean A y B dos conjuntos. Se llama *correspondencia* (binaria) entre A y B a cualquier subconjunto R del producto cartesiano $A \times B$, es decir, $R \subseteq A \times B$. En el caso particular $A = B$ se habla de *relación (binaria) sobre* A.

Algunos autores no mencionan el término "correspondencia" y hablan también de "relación entre A y B". Nótese que los conjuntos $\varnothing$ y $A \times B$ (el vacío y el total) son siempre (de manera trivial) correspondencias entre A y B.

El adjetivo "binaria" alude al hecho de ser subconjunto del producto cartesiano de *dos* conjuntos. Nosotros vamos a trabajar siempre con correspondencias y relaciones *binarias*, por lo que omitiremos a partir de ahora la palabra "binaria" y escribiremos simplemente "correspondencia" o "relación".

Sean $a \in A$, $b \in B$, y sea R una correspondencia entre A y B. Se dice que *a y b están relacionados mediante R* si $(a,b) \in R$; se escribe también aRb.

Ejemplos. (1) Sean los conjuntos $A = \{0,3,5\}$ y $B = \{s,t,v\}$. El conjunto

$$R = \{(0,s),(5,v)\} \subseteq A \times B$$

es una correspondencia entre A y B. El conjunto

$$S = \{(3,s),(3,v),(5,s),(5,t),(5,v)\} \subseteq A \times B$$

es otra correspondencia entre A y B.
(2) Sea A un conjunto. La relación $\mathrm{id}_A := \{(a,a) \in A \times A : a \in A\}$ se llama la *relación identidad* sobre A.

Sean A, B dos conjuntos y $R \subseteq A \times B$ una correspondencia entre ellos. Se define el *dominio* de R como

$$\mathrm{Dom}(R) := \{a \in A : \text{ existe } b \in B \text{ tal que } (a,b) \in R\},$$

y la *imagen* de R como

$$\mathrm{Im}(R) := \{b \in B : \text{ existe } a \in A \text{ tal que } (a,b) \in R\}.$$

En el ejemplo anterior, $\mathrm{Dom}(R) = \{0,5\}$, $\mathrm{Im}(R) = \{s,v\} \subsetneq B$, $\mathrm{Dom}(S) = \{3,5\}$ y $\mathrm{Im}(S) = \{s,v,t\} = B$.

El conjunto A se llama conjunto de partida o inicial, y B se llama conjunto de llegada o final. Más aún, si R es una correspondencia entre A y B, dado $A' \subseteq A$, se

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

denomina *imagen* de A' por R al conjunto

$$R(A') = \{b \in B : \exists a \in A' \text{ con } (a,b) \in R\}.$$

Nótese que $R(A) = \mathrm{Im}(R)$. Las siguientes propiedades son de comprobación inmediata:

Teorema 4.1. *Sea R una correspondencia entre A y B, y sean $A', A'' \subseteq A$. Se verifica:*

(a) *Si $A' \subseteq A''$, entonces $R(A') \subseteq R(A'')$.*
(b) $R(A' \cup A'') = R(A') \cup R(A'')$
(c) $R(A' \cap A'') \subseteq R(A') \cap R(A'')$.

Por ejemplo, si $A = \{0,3,5\}$, $A' = \{0,3\}$, $A'' = \{3,5\}$, $B = \{s,t,v\}$ y consideramos la relación $T = \{(3,s),(0,v),(5,v),(5,t)\}$, entonces se comprueba que $T(A') \cap T(A'') = \{s,v\} \cap \{s,v,t\} = \{s,v\}$ pero $T(A' \cap A'') = T(\{3\}) = \{s\}$, luego no tiene por qué ser cierta la igualdad en (c).

La siguiente clasificación de relaciones binarias es esencial en matemáticas:

Definición. Sean A un conjunto y R una relación sobre A. Se dice que R es

- *reflexiva* si se verifica que $(x,x) \in R$ para todo $x \in A$;
- *simétrica* si se cumple que

$$\forall x, y \in A : (x,y) \in R \longrightarrow (y,x) \in R;$$

- *antisimétrica* si se satisface que

$$\forall x, y \in A : (x,y) \in R \ \wedge \ (y,x) \in R \ \longrightarrow \ x = y;$$

- *transitiva* cuando

$$\forall x, y, z \in A : (x,y) \in R \ \wedge \ (y,z) \in R \ \longrightarrow \ (x,z) \in R;$$

- *conexa* si se cumple:

$$\forall x, y \in A : (x,y) \in R \ \vee \ (y,x) \in R.$$

Ejemplos. Sea el conjunto $A = \{1,2,3,4,5\}$.

(1) La relación $R_1 = \{(1,1),(1,2),(1,3),(2,2),(3,3)\}$ sobre A no es reflexiva, pues por ejemplo el par $(4,4)$ no aparece. Se puede hacer reflexiva añadiendo los dos pares $(4,4),(5,5)$.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

(2) La relación $R_2 = \{(1,1),(1,2),(1,3),(3,3)\}$ no es simétrica, pues estando el par $(1,2)$, no aparece el par $(2,1)$. Se puede hacer simétrica añadiendo los pares $(2,1)$ y $(3,1)$.

(3) La relación $R_3 = \{(1,1),(5,2),(2,5)\}$ no es antisimétrica, pues aunque $(2,5)$ y $(5,2)$ son elementos de R_3, esto no implica la igualdad $5 = 2$.

(4) La relación $R_4 = \{(1,1),(2,5)\}$ sí es antisimétrica. Justifiquémoslo. Sea p la proposición $(2,5) \in R_4$, sea q la proposición $(5,2) \in R_4$ y sea r la proposición $2 = 5$. La propiedad antisimétrica se reescribe como la proposición compuesta $p \wedge q \to r$.

Sabemos que la proposición p es cierta (pues $(2,5) \in R_4$), mientras que tanto q como r son falsas (ya que $(5,2) \notin R_4$ y además $2 \neq 5$). La pregunta por el valor de verdad de la implicación anterior es equivalente a preguntarse si R_4 es antisimétrica. ¿Cuál es entonces el valor de verdad de la implicación en $p \wedge q \to r$? Echemos un vistazo a las tablas de verdad de $\wedge$ y de $\to$:

$\mathbf{p}$	$\mathbf{q}$	$\mathbf{r}$	$\mathbf{p \wedge q}$	$\mathbf{(p \wedge q) \to r}$
v	f	f	f	**v**

Observamos que la implicación es verdadera, lo que quiere decir que la relación R_4 es antisimétrica.

(5) ¿Es la relación R_4 del apartado anterior transitiva? Un razonamiento similar al efectuado en (4) responde a la pregunta afirmativamente.

(6) La relación $R_5 = \{(2,2),(1,5),(5,1),(4,4)\}$ no es transitiva, pues por ejemplo no contiene al elemento $(1,1)$ estando $(1,5)$ y $(5,1)$.

(7) La relación $R_6 = \varnothing$ no es reflexiva (falta por ejemplo el elemento $(1,1)$), pero es simétrica, antisimétrica y transitiva.

Para ver la simetría, empleemos de nuevo una pizca de lógica proposicional. Sean $x, y \in A$, sea p la proposición $(x,y) \in R_6$, y q la proposición $(y,x) \in R_6$. Se trata de analizar el valor de verdad de la implicación $p \to q$, sabiendo que tanto p como q son falsas, lo que es, como sabemos, verdadero:

$\mathbf{p}$	$\mathbf{q}$	$\mathbf{p \to q}$
f	f	**v**

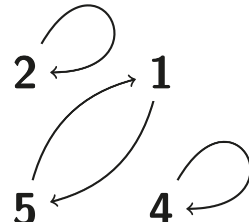
Análogamente se comprueba que R_6 es antisimétrica y transitiva.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

(8) La relación $R_7 = A \times A$ es reflexiva, simétrica y transitiva, pero no antisimétrica.

Nota. Que una relación sea antisimétrica no quiere decir *no simétrica*. De hecho, existen relaciones R, digamos sobre un conjunto A, que son a la vez simétricas y antisimétricas, como la relación de igualdad, o la relación $R = \varnothing$ (cf. (7) del ejemplo anterior); o que no son simétricas ni antisimétricas, como la divisibilidad de los números enteros, que trataremos después; o que son antisimétricas pero no simétricas, como la relación $\leq$; o que son simétricas pero no antisimétricas, como la relación $R = A \times A$ (ver (8) en el ejemplo anterior).

Una relación sobre un conjunto finito se puede representar mediante un diagrama sagital, en el que las relaciones entre los elementos se visualizan con flechas. Por ejemplo, en (6) del ejemplo anterior la relación R_5 se representa por el diagrama sagital



Veamos en último lugar cómo las relaciones se pueden revertir y también vincular o enlazar o *componer* unas con otras siempre que sus conjuntos definitorios sean compatibles:

Definición. Sean A, B, C tres conjuntos. Sean R una correspondencia entre A y B, y S una correspondencia entre B y C.

(a) La correspondencia entre B y A

$$\{(b,a) \in B \times A : (a,b) \in R\} \subseteq B \times A$$

se llama correspondencia *recíproca* o *inversa* de R, y se denota por R^{-1}. Es obvio que $(R^{-1})^{-1} = R$.

(b) La correspondencia

$$S \circ R := \{(a,c) \in A \times C : \exists\, b \in B \text{ con } (a,b) \in R \wedge (b,c) \in S\} \subseteq A \times C$$

se llama *composición* de R con S.

Ejemplos. (1) El conjunto $R = \{(x,y) \in \mathbb{N}^2 : x \leq y\}$ es una relación en $\mathbb{N}$. Su inversa es

$$R^{-1} = \{(y,x) \in \mathbb{N}^2 : (x,y) \in R\} = \{(y,x) \in \mathbb{N}^2 : x \leq y\} = \{(y,x) \in \mathbb{N}^2 : y \geq x\}.$$

(2) Sean $A = \{a,b,c,d\}$, $B = \{1,2,3\}$ y $C = \{w,x,y,z\}$, así como las correspondencias $R = \{(b,1),(c,2),(d,1)\}$ entre A y B, y $S = \{(3,x),(2,w),(1,y),(1,z)\}$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

entre B y C. Entonces se tiene que la composición

$$S \circ R = \{(b,y),(b,z),(c,w),(d,y),(d,z)\} \subseteq A \times C$$

de S con R es una correspondencia entre A y C. No se puede formar la composición $R \circ S$, pero teniendo en cuenta que $R^{-1} = \{(1,b),(2,c),(1,d)\} \subseteq B \times A$ y que $S^{-1} = \{(x,3),(w,2),(y,1),(z,1)\} \subseteq C \times B$, se tiene que

$$R^{-1} \circ S^{-1} = \{(w,c),(y,b),(y,d),(z,b),(z,d)\}.$$

Obsérvese en este ejemplo que $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$. Este hecho es general, como muestra el resultado siguiente.

Teorema 4.2. *Dadas las correspondencias R de A en B y S de B en C, se verifica que* $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

Demostración. Basta observar la siguiente cadena de igualdades:

$$\begin{aligned}(S \circ R)^{-1} =& \{(c,a) \in C \times A : (a,c) \in S \circ R\} \\ =& \{(c,a) \in C \times A : \exists b \in B \text{ con } (a,b) \in R \wedge (b,c) \in S\} \\ =& \{(c,a) \in C \times A : \exists b \in B \text{ con } (c,b) \in S^{-1} \wedge (b,a) \in R^{-1}\} \\ =& R^{-1} \circ S^{-1}.\end{aligned}$$

Con ello el resultado queda probado. □

Relaciones de orden. El lenguaje de las relaciones permite introducir la noción de orden en matemáticas. Una relación R sobre un conjunto A se dice que es *de orden* si verifica las propiedades reflexiva, antisimétrica y transitiva.

A veces se emplea la más sugestiva notación "$\preceq$" en lugar de "R"; en tal caso, si dos elementos $a, b \in A$ están relacionados se escribirá $a \preceq b$ en lugar de aRb; se dirá entonces que "a precede a b por la relación R", o que "b sigue a a"; en ocasiones se dice que "a es menor o igual que b". Es útil definir también:

$$\begin{aligned} a \succeq b :\Longleftrightarrow & b \preceq a \\ a \prec b :\Longleftrightarrow & (a \preceq b) \wedge (a \neq b) \\ a \succ b :\Longleftrightarrow & b \prec a \end{aligned}$$

Una relación de orden R se dice *total* si además es conexa, es decir, si verifica

- ⋄ $\forall a,b$: $(a,b) \in R \vee (b,a) \in R$.

Un *conjunto parcialmente ordenado* o *poset*[1] es un conjunto en el que se ha definido una relación de orden. Si el orden es total se habla de conjunto *totalmente*

[1] Del inglés *partially ordered set.*

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

ordenado. Se empleará la notación $(A, \preceq)$ para expresar que el conjunto A está (total o parcialmente) ordenado por la relación de orden "$\preceq$".

Los conjuntos ordenados finitos admiten una representación gráfica llamada *diagrama de Hasse,*[2] que es una simplificación del diagrama sagital de la relación de orden subyacente. En los diagramas de Hasse se dibuja una arista ascendente entre dos elementos sólo si el primero precede al segundo por la relación, sin que haya otros elementos intermedios; por tanto, se eliminan de la representación todas las aristas que se deducen de la reflexividad (es decir, los lazos de un elemento en sí mismo) y de la transitividad de la relación de orden.

Ejemplos. (1) Sea A un conjunto y consideremos la relación identidad

$$R = \mathrm{id}_A = \{(a,a) : a \in A\} \subseteq A \times A.$$

En otras palabras, para todos $a, b \in A$ se verifica

$$aRb \quad \text{si y solamente si} \quad a = b.$$

Esto significa que R nos ofrece la igualdad "$=$" sobre el conjunto A. Esta relación es de orden, ya que:

- R es reflexiva: se cumple trivialmente que $(a,a) \in R = \mathrm{id}_A$ para cualquier $a \in A$.
- R es antisimétrica: supuesto que si $(a,b) \in R$ y $(b,a) \in R$, se tiene trivialmente la igualdad $a = b$.
- R es transitiva: para cualesquiera $a,b,c \in A$ tales que $(a,b) \in R$ (lo que significa $a = b$), y con $(b,c) \in R$ (lo que quiere decir que $b = c$), obtenemos $a = b = c$, en particular $a = c$, lo que implica $(a,c) \in R$.

(2) Sea A un conjunto, y $\mathscr{P}(A)$ su conjunto potencia. Consideremos la relación

$$R := \{(X,Y) : X \subseteq Y\} \subseteq \mathscr{P}(A) \times \mathscr{P}(A).$$

La relación R es de orden, pues

- es reflexiva: para cualquier $X \in \mathscr{P}(A)$ se tiene $(X,X) \in R$, ya que se verifica siempre $X \subseteq X$.
- es antisimétrica: Que $(X,Y) \in R$ y $(Y,X) \in R$ significa que se tienen las contenciones $X \subseteq Y$ y $Y \subseteq X$, es decir la igualdad $X = Y$.
- es transitiva: Supongamos que $(X,Y) \in R$ y que $(Y,Z) \in R$ para todo $X,Y,Z \in \mathscr{P}(A)$. Esto quiere decir tanto que $X \subseteq Y$ como que $Y \subseteq Z$, que implica $X \subseteq Z$, es decir, $(X,Z) \in R$.

[2] Por el alemán Helmut HASSE (1898–1979). Aunque, de acuerdo con su discípulo G. Pickert, Hasse no estaba muy contento de que su nombre se relacionara con un objeto tan simple, cf. [**BT**].

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Las relaciones de orden juegan también un papel muy importante. En ellas se distinguen los siguientes elementos (tradicionalmente llamados) notables:

Definición. Sea $(A, \preceq)$ un conjunto ordenado, y sea $X \subseteq A$.

(a) Un elemento $a \in A$ se llama *cota superior* de X si $x \preceq a$ para todo $x \in X$.
(b) Un elemento $a \in A$ se llama *cota inferior* de X si $a \preceq x$ para todo $x \in X$.
(c) El conjunto X se dice que está *acotado superiormente* si posee cota superior.
(d) El conjunto X se dice que está *acotado inferiormente* si posee cota inferior.
(e) El conjunto X se llama *acotado* si lo está superior e inferiormente.

Las cotas superiores e inferiores pueden no ser únicas, pero se pueden elegir las más ajustadas:

Definición. Se llama *supremo* o *extremo superior* de X a la menor de las cotas superiores, caso de que exista; se escribe $\sup X$. Se llama *ínfimo* o *extremo inferior* de X a la mayor de las cotas inferiores, caso de que exista; se escribe $\inf X$. Nótese que ni $\sup X$ ni $\inf X$ tienen por qué pertenecer a X. Cuando esto sucede reciben nombres especiales:

(a) Si el supremo de X es un elemento de X se le llama *máximo*, y se denota por $\text{máx}\, X$.
(b) Si el ínfimo de X es elemento de X se le llama *mínimo*, y se denota por $\text{mín}\, X$.

Estas cotas más ajustadas sí que son, de existir, únicas:

Teorema 4.3. *Sea $(A, \preceq)$ un conjunto ordenado. El supremo y el ínfimo de A, caso de existir, son únicos.*

Demostración. Veamos que el supremo, si existe, es único. Supongamos que existieran α, β dos supremos de A; en particular son cotas superiores de A. Por ser α supremo, es menor que cualquier otra cota, esto es, $\alpha \preceq \beta$. Por ser β supremo, es menor que cualquier cota y así $\beta \preceq \alpha$. La antisimetría implica la igualdad $\alpha = \beta$. Hemos demostrado: si A admitiera dos supremos, han de coincidir, lo que prueba la unicidad del supremo. Mutatis mutandis se prueba la unicidad del ínfimo. □

Ejemplo. Sea $\mathbb{R}$ el cuerpo de los números reales dotado del orden usual $\leq$. Sea $I := \{x \in \mathbb{R} : 0 \leq x < 1\}$, es decir, el intervalo semiabierto $[0, 1[$. Este conjunto está acotado superiormente: los elementos en

$$\{x \in \mathbb{R} : x \geq 1\}$$

son todos cotas superiores de I. La menor de las cotas superiores es 1, pero $1 \notin I$. Por ello 1 es el supremo de I, pero no es máximo.

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

Por otro lado, el conjunto I también está acotado inferiormente. De hecho, todos los elementos del conjunto

$$\{x \in \mathbb{R} : x \leq 0\}$$

son cotas inferiores de I. La mayor de ellas es 0, y $0 \in I$. Entonces 0 es el ínfimo de I, y también su mínimo. Como I está acotado tanto superior como inferiormente, está acotado.

Definición. Sean $(A, \preceq)$ un conjunto ordenado, y sea $\varnothing \neq X \subseteq A$ con $x \in X$. El elemento x se llama *maximal* de X (respecto de $\preceq$) si

$$\forall\, y \in X : (x \preceq y \longrightarrow x = y).$$

Por otro lado, x se llama elemento *minimal* de X (respecto de $\preceq$) si

$$\forall\, y \in X : (y \preceq x \longrightarrow y = x).$$

Nótese que los elementos maximales y minimales no tienen por qué ser únicos.

Ejemplos. (1) Para el primer ejemplo (y para el siguiente) necesitamos formalizar la noción de divisibilidad de números enteros; es fácil: dados $m, n \in \mathbb{Z}$, se dice que n divide a m, y se escribe $n \mid m$, si existe $z \in \mathbb{Z}$ tal que $m = nz$. Tal como la hemos expresado, esta relación no es de orden, pues no es antisimétrica: por ejemplo, tomando $3, -3 \in \mathbb{Z}$, ocurre que $3 \mid -3$ y $-3 \mid 3$ pero $3 \neq -3$. El problema se arregla restringiendo la definición al conjunto $\mathbb{N}$: dos números *naturales* x, y están relacionados mediante R si y solamente si el uno divide al otro, es decir,

$$xRy \iff x \mid y$$

(en la otra notación: $x \preceq y \iff x \mid y$). Esta relación es una relación de orden (¡ejercicio!).

(2) Sea X el conjunto de todos los números naturales que dividen a 36 salvo él mismo y la unidad, esto es, $X = \{2, 3, 4, 6, 9, 12, 18\} \subseteq \mathbb{N}$. Este conjunto está parcialmente ordenado respecto de la relación de orden R definida por la "divisibilidad" de números naturales vista en (1). Los elementos minimales son 2 y 3, ya que

- para todo $y \in X$ con $y|3$ se tiene solamente $y = 3$;
- para todo $y \in X$ con $y|2$ se tiene solamente $y = 2$.

Los elementos maximales son 12 y 18, ya que

- para todo $y \in X$ con $12|y$ se tiene solamente $y = 12$;
- para todo $y \in X$ con $18|y$ se tiene solamente $y = 18$.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

(3) Sea $Y = \{1,2,5,7,10,14,35,70\} \subseteq \mathbb{N}$ el conjunto de todos los números naturales que dividen a 70, ordenado por la relación dada por la divisibilidad. En este caso existe un único elemento maximal, el 70, y un único minimal, el 1.

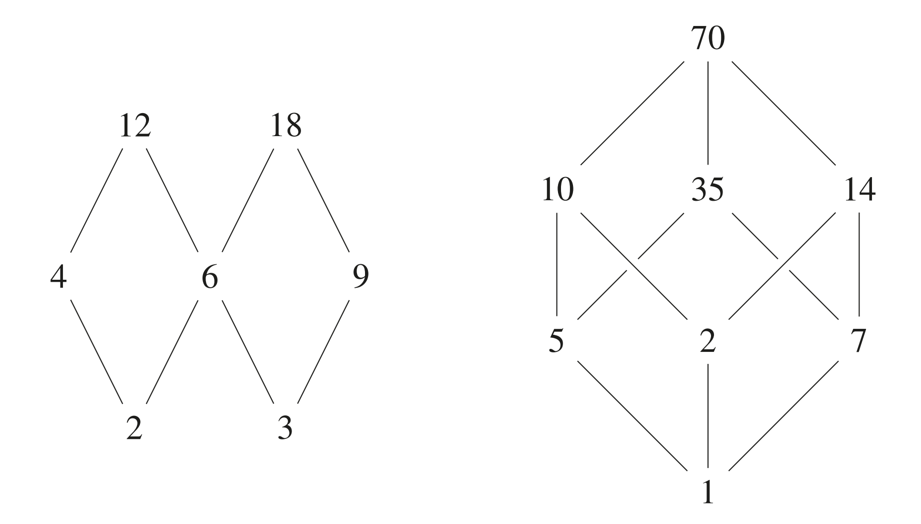


FIGURE 1. Diagramas de Hasse de los posets X e Y en (1) y (2)

(4) Se define $\mathscr{M} := \mathscr{P}(\mathbb{N}) \setminus \{\mathbb{N}, \varnothing\}$. Se comprueba fácilmente que $\mathscr{M}$ es un conjunto parcialmente ordenado por la inclusión "$\subseteq$". Se buscan los elementos maximales y minimales de $\mathscr{M}$. Por una parte, como $\varnothing \notin \mathscr{M}$, ninguno de los conjuntos de la forma $\{n\} \in \mathscr{M}$ (para un $n \in \mathbb{N}$ arbitrario) puede ser precedido por un elemento de $\mathscr{M}$ con respecto a "$\subseteq$", por tanto, son todos ellos elementos minimales con respecto a este orden. Un razonamiento análogo nos permite deducir que los elementos maximales de $\mathscr{M}$ son los de la forma $\mathbb{N} \setminus \{n\}$, con $n \in \mathbb{N}$.

(5) Sea $\mathscr{P}(\mathbb{N}) \setminus \{\mathbb{N}\}$ y el orden dado por la inclusión. En este caso $\varnothing$ es el único elemento minimal, y los maximales son todos los de la forma $\mathbb{N} \setminus \{n\}$, para todo $n \in \mathbb{N}$.

(6) Por último, consideremos $\mathscr{P}(\mathbb{N}) \setminus \{\varnothing\}$. Ahora todos los conjuntos $\{n\}$ son minimales, pero $\mathbb{N}$ es el único elemento maximal con respecto al orden dado por la inclusión.

[Big] Biggs, N.L.: Discrete Mathematics. Second ed. Oxford U.P., 2004
[BT] Beutelspacher, A., Törner, G.: Interview mit Professor Dr. Günter Pickert. Mitteilungen der DMV, 23 (1), 2015, 48–58
[Cab] Caballero Roldán, Rafael et al.: Matemática Discreta para Informáticos. Ejercicios resueltos. Pearson/Prentice Hall, 2007
[Conr] Conradie, W., Goranko, V.: Logic and Discrete Mathematics. A concise introduction. Wiley, 2015
[FG] Ferrando, J.C., Gregori, V.: Matemática Discreta. 2. ed. Reverté, 2002
[Gall] Gallier, J.: Discrete Mathematics. Springer, 2011
[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3. ed. McGraw Hill, 2007
[Pla] Pla i Carrera, J.: Introducció a la metodologia de la Matemàtica. Universitat de Barcelona, 2006
[SchWie] Schafmeister, O., Wiebe, H.: Grundzüge der Algebra. B.G. Teubner, 1978
[StW] Storch, U. und Wiebe, H.: Lehrbuch der Mathematik, Band 2. Spektrum, Heidelberg, 1999
[Wall2] Wallis, W.D.: A beginner's guide to discrete mathematics. Second edition. Birkhäuser, 2012

Capítulo 5. Conjuntos cociente

Este capítulo complementa el anterior, y trata de una clase de relaciones muy importantes que ayudan en el problema de la *clasificación* de entidades matemáticas (que es una de sus grandes cuestiones). Para clasificar, tomamos los elementos de un conjunto y nos aseguramos de que podemos hacer "paquetes" bien definidos en los que repartimos, según criterios dados, los elementos originales. Por ejemplo, consideremos el conjunto de los habitantes de Castellón de la Plana, y sobre él definamos la relación "tener los mismos padres":

$$xRy \quad :\Longleftrightarrow \quad x \text{ tiene los mismos padres que } y.$$

Esta relación "parte" la población de Castellón en grupúsculos, en cada uno de los cuales están las personas que son hermanos. Esta idea intuitiva nos lleva a la definición de *partición* de un conjunto:

Definición. Sea M un conjunto no vacío. Una *partición* de M es un conjunto $\mathscr{M}$ cuyos elementos son subconjuntos de M tales que

(a) los conjuntos en $\mathscr{M}$ son no vacíos;
(b) los conjuntos de $\mathscr{M}$ son disjuntos dos a dos, es decir

$$\forall N, N' \in \mathscr{M} : \; N \neq N' \implies N \cap N' = \varnothing.$$

(c) con todos los conjuntos ha de poder cubrirse M, es decir,

$$\bigcup_{N \in \mathscr{M}} N = M.$$

Si no se exige la segunda condición, se habla de *recubrimiento* de M.

Las relaciones en las que estamos interesados en este capítulo nos ofrecerán una fuente generadora de particiones:

Definición. Una relación se dice que es *de equivalencia* si cumple las propiedades reflexiva, simétrica y transitiva.

Efectivamente, la relación "tener los mismos padres" es de equivalencia. Veremos más ejemplos, pero antes hagamos algunas observaciones.

Dada una relación de equivalencia R sobre un conjunto A, que un elemento $a \in A$ esté relacionado con un elemento $b \in B$ se consigna con diversas notaciones, todas ellas arraigadas en la literatura:

$(a,b) \in R$, aRb, $a \sim_R b$ o simplemente $a \sim b$ si la relación es clara en el contexto.

Para un elemento $a \in A$, se define la *clase de equivalencia* de a por la relación R, y se denota por $[a]_R$, o simplemente por $[a]$ si el riesgo de confusión no acecha, al conjunto

$$[a] := \{x \in A : (x,a) \in R\} = \{x \in A : xRa\} = \{x \in A : x \sim_R a\}.$$

Nótese que $[a] \subseteq A$, y que $a \in [a]$. El conjunto de las clases de equivalencia se denomina *conjunto cociente* de la relación R sobre el conjunto A; se denota A/R. (Obsérvese que los elementos del conjunto cociente son, a su vez, conjuntos). En otras palabras,

$$A/R = \{[a] : a \in A\}.$$

Si la relación se está denotando por $\sim$ no es infrecuente escribir $A/\sim$. Veamos algunos ejemplos.

Ejemplos. (1) Sea A un conjunto y consideremos la relación identidad

$$R = \mathrm{id}_A = \{(a,a) : a \in A\} \subseteq A \times A.$$

Dicho de otra manera, para todos $a,b \in A$ se verifica

$$aRb \quad \text{si y solamente si} \quad a = b.$$

Esto significa que R nos ofrece la igualdad "=" sobre el conjunto A. Esta relación es de equivalencia, pues:

- R es reflexiva: se cumple trivialmente que $(a,a) \in R = \mathrm{id}_A$ para cualquier $a \in A$.
- R es simétrica: supuesto que $(a,b) \in R$, se tiene la igualdad $a = b$, y así se cumple también $(b,a) \in R$.
- R es transitiva: para cualesquiera $a,b,c \in A$ tales que $(a,b) \in R$ (lo que significa $a = b$), y con $(b,c) \in R$ (lo que quiere decir que $b = c$), obtenemos $a = b = c$, en particular $a = c$, lo que implica $(a,c) \in R$.

Dado $a \in A$, es obvio que su clase de equivalencia está formada sólo por a, es decir,

$$[a] = \{x \in A : xRa\} = \{x \in A : x = a\} = \{a\}.$$

(2) Sea $\mathfrak{P}$ el conjunto de las proposiciones simples. Para cada $p,q \in \mathfrak{P}$ se define la relación "ser lógicamente equivalente" (denotada por $\equiv$) como sigue:

$$p \equiv q \;:\Longleftrightarrow\; p \Leftrightarrow q.$$

Esta relación es de equivalencia:

(a) es reflexiva: para todo $p \in \mathfrak{P}$ es $p \equiv p$, ya que $p \Leftrightarrow p$;
(b) es simétrica: para cualesquiera $p,q \in \mathfrak{P}$, si $p \equiv q$ se tiene que $(p \Leftrightarrow q) \Longrightarrow (q \Leftrightarrow p)$, es decir, $q \equiv p$.
(c) transitiva: para cualesquiera tres $p,q,r \in \mathfrak{P}$,si $p \equiv q$ y $q \equiv r$, entonces $p \equiv r$, puesto que $(p \Leftrightarrow q) \wedge (q \Leftrightarrow r) \Longrightarrow (p \Leftrightarrow r)$.

(3) Para cualesquiera $x,y \in \mathbb{Z}$ se define una relación R entre ellos como sigue: se dice que x está relacionado con y, es decir xRy, si $x^2 - y^2 = x - y$. Esta relación es de equivalencia, pues es

(a) reflexiva: para todo $x \in \mathbb{Z}$ es xRx ya que $x^2 - x^2 = 0 = x - x$;
(b) simétrica: para cualesquiera $x,y \in \mathbb{Z}$, si xRy se tiene que $x^2 - y^2 = x - y$, que es lo mismo que escribir $y^2 - x^2 = y - x$, es decir yRx;
(c) transitiva: para cualesquiera tres $x,y,z \in \mathbb{Z}$, las condiciones xRy e yRz se traducen por definición en sendas ecuaciones $x^2 - y^2 = x - y$ e $y^2 - z^2 = y - z$. Ahora bien, estas dos ecuaciones se pueden sumar, y se obtiene:

$$\begin{array}{rcl} x^2 - y^2 & = & x - y \\ +[y^2 - z^2 & = & y - z] \\ \hline x^2 - y^2 + y^2 - z^2 & = & x - y + y - z, \end{array}$$

es decir, $x^2 - z^2 = x - z$, lo que quiere decir que xRz y así la transitividad de la relación queda probada.

Dado $x \in \mathbb{Z}$, su clase de equivalencia viene dada por el conjunto

$$[x] = \{y \in \mathbb{Z} : xRy\} = \{y \in \mathbb{Z} : x^2 - y^2 = x - y\}$$

Nótese que

$$x^2 - y^2 = (x+y)(x-y),$$

por lo que cuando $x \neq y$ (es decir, cuando $x - y \neq 0$) se puede dividir ambos miembros de la igualdad "$x^2 - y^2 = x - y$" por $x - y$, y queda $x + y = 1$, o, lo que es lo mismo, $y = 1 - x$. Recuérdese que se ha de tratar aparte el caso $x = y$. Así se obtiene

$$[x] = \{y \in \mathbb{Z} : y = x\} \cup \{y \in \mathbb{Z} : x \neq y \wedge y = 1 - x\},$$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

o, escrito de manera más compacta

$$[x] = \{x, 1-x\}.$$

Una simple inspección muestra que $[0] = [1], [2] = [-1], [3] = [-2], \dots$ y en general $[n] = [-(n-1)]$ para todo $n \in \mathbb{N}$. Por tanto, el conjunto cociente de $\mathbb{Z}$ por la relación R es

$$\mathbb{Z}/R = \Big\{[1], [2], [3], [4], \dots\Big\} = \Big\{[n] : n \in \mathbb{N}, n \geq 1\Big\}.$$

Las clases de equivalencia definen una partición del conjunto sobre el que se define la relación de equivalencia:

Teorema 5.1. *Sea R una relación de equivalencia sobre un conjunto A, entonces:*

(a) $[a] \neq \varnothing$;
(b) $A = \bigcup_{a \in A} [a]$;
(c) *Son equivalentes:*
  (i) $[a] = [b]$;
  (ii) $[a] \cap [b] \neq \varnothing$;
  (iii) $a \sim b$.

Demostración. Es evidente que $a \in [a]$ al ser la relación reflexiva; también es evidente (b). En cuanto a (c), basta observar:
(i) $\Longrightarrow$ (ii): Como $a \in [a] = [b]$, entonces $a \in [a] \cap [b]$.
(ii) $\Longrightarrow$ (iii): Sea $x \in [a] \cap [b]$, entonces $x \sim a$ y $x \sim b$, y por la simetría de la relación $a \sim x$. La transitividad de la misma permite concluir que $a \sim b$.
(iii) $\Longrightarrow$ (i): Probemos en primer lugar la inclusión $[a] \subseteq [b]$; sea para ello $x \in [a]$, entonces $x \sim a$ y como por hipótesis $a \sim b$, entonces la transitividad asegura que $x \sim b$, es decir, $x \in [b]$. Además, por la simetría, si $a \sim b$ entonces $b \sim a$, de donde se sigue la otra contención $[b] \subseteq [a]$, y con todo la igualdad $[a] = [b]$. □

Las relaciones de equivalencia permiten la construcción formal de conjuntos de números que conocemos desde la escuela, como los enteros y las fracciones, y también otros nuevos. En lo que resta de capítulo trataremos sucintamente estas cuestiones.

Comencemos construyendo $\mathbb{Z}$ por medio de una relación de equivalencia sobre el conjunto $\mathbb{N} \times \mathbb{N}$ basado en la observación siguiente:

Cualquier número entero z se puede escribir como diferencia $a - b$ entre dos números naturales a y b, *no* de forma única.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Efectivamente, sucede que un mismo número entero z se escribe de al menos dos formas distintas

$$z = a - b = c - d.$$

(Piénsese, por ejemplo, en $-3 = 4 - 7 = 6 - 9$). La idea es identificar el número entero z con el par (a,b) y, en realidad, con todos los pares cuya diferencia sea z. Es decir, queremos hacer paquetes de acuerdo a la siguiente relación:

$$(a,b) \sim (c,d) :\Longleftrightarrow a + d = b + c.$$

Esta relación es de equivalencia:

(a) es reflexiva: para todo $(a,b) \in \mathbb{N} \times \mathbb{N}$ es $a + b = b + a$, es decir, $(a,b) \sim (a,b)$;
(b) es simétrica: si $(a,b) \sim (c,d)$, entonces $a + d = b + c \iff c + b = d + a$, es decir, $(c,d) \sim (a,b)$;
(c) es transitiva: si $(a,b) \sim (c,d)$ y $(c,d) \sim (e,f)$, entonces $a + d = b + c$ y $c + f = d + e$; sumando ambas igualdades y simplificando $d + c$ queda que $a + f = b + e$, es decir, $(a,b) \sim (e,f)$.

La clase de equivalencia de un par (a,b) es

$$[(a,b)] = \{(x,y) : (x,y) \sim (a,b)\} = \{(x,y) : x+b = y+a\} = \{(x,y) : a-b = x-y\}.$$

Está claro: la clase de equivalencia de (a,b) contiene todos los pares (x,y) tales que la diferencia $x - y$ sea la misma que $a - b$, como queríamos. El conjunto cociente $\mathbb{N} \times \mathbb{N}/\sim$ lo denotaremos $\mathbb{Z}$. Por ejemplo, el número entero 3 es la clase de equivalencia $[(3,0)]$, el número -4 es la clase de equivalencia $[(0,4)]$, etc. Que esta construcción es compatible con las operaciones con números enteros que conocemos es otra historia, que se deja como ejercicio.

De una manera análoga se puede construir $\mathbb{Q}$: sobre el producto cartesiano $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ se define la siguiente relación:

$$(a,b) \sim (c,d) :\Longleftrightarrow ad = bc.$$

Se comprueba que es una relación de equivalencia y la clase de equivalencia $[(a,b)]$ es la fracción a/b. De hecho, la condición $ad = bc$ asegura que dos fracciones a/b y c/d tales que

$$\frac{a}{b} = \frac{c}{d}$$

están en la misma clase de equivalencia:

$$[(a,b)] = \{(x,y) : (x,y) \sim (a,b)\} = \{(x,y) : xb = ya\} = \left\{(x,y) : \frac{x}{y} = \frac{a}{b}\right\}.$$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Cerramos el capítulo con una construcción nueva basada en la relación “tener el mismo resto” al dividir por un número natural prefijado. Precisemos. Sea $n \in \mathbb{N}$, $n > 1$. Para cualesquiera $a, b \in \mathbb{Z}$ denotamos

$$a \equiv b \mod n$$

(se lee: “a es congruente con b módulo n”) si y sólo si la división de a y de b por n arroja el mismo resto $r \in \mathbb{N}$, con $0 \leq r < n$. Formalmente:

$$a \equiv b \mod n \quad :\Longleftrightarrow \exists k \in \mathbb{Z} : a = kn + b.$$

Ello define una relación R sobre $\mathbb{Z}$ que es reflexiva, simétrica y transitiva, luego es una relación de equivalencia:

(a) es reflexiva, es decir, para cualquier $a \in \mathbb{Z}$ es a es congruente módulo n consigo mismo, pues efectivamente existe un entero k tal que $a = kn + a$: basta tomar $k = 0$.

(b) es simétrica, ya que si existe $k \in \mathbb{Z}$ tal que $a = kn + b$, entonces también existe un $k' \in \mathbb{Z}$ tal que $b = k'n + a$, pues basta tomar $k' := -k$.

(c) es transitiva, y para verlo tomemos $a, b, c \in \mathbb{Z}$ y supongamos que a es congruente con b módulo n y que b es congruente con c módulo n, es decir, que existen $k_1 \in \mathbb{Z}$ y $k_2 \in \mathbb{Z}$ tales que

$$a = k_1 n + b \text{ y } b = k_2 n + c.$$

Se puede entonces substituir el valor de b de la segunda igualdad en la primera y operar:

$$a = k_1 n + (k_2 n + c) = (k_1 + k_2)n + c,$$

y como $k_1 + k_2 \in \mathbb{Z}$, hemos demostrado que a es congruente con c módulo n.

Para esta relación de equivalencia R, el conjunto cociente $\mathbb{Z}/R$ se denota por $\mathbb{Z}_n$ (otros usos imponen las escrituras $\mathbb{Z}/(n)$ o también $\mathbb{Z}/\mathbb{Z}n$), y está formado por n clases de equivalencia

$$[0], [1], [2], \ldots, [n-1],$$

distintas dos a dos, donde cada clase de equivalencia es a su vez el conjunto

$$[a] = \{a + kn : k \in \mathbb{Z}\}.$$

Para esta relación de congruencia, las clases de equivalencia también se llaman *clases modulares* (módulo n).

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

[Big] Biggs, N.L.: Discrete Mathematics. Second ed. Oxford U.P., 2004

[Cab] Caballero Roldán, R. et al.: Matemática Discreta para Informáticos. Ejercicios resueltos. Pearson/Prentice Hall, 2007

[Conr] Conradie, W., Goranko, V.: Logic and Discrete Mathematics. A concise introduction. Wiley, 2015

[FG] Ferrando, J.C., Gregori, V.: Matemática Discreta. 2. ed. Reverté, 2002

[GOV] Galindo Pastor, C., Orús Báguena, M.P., Vindel Cañas, M.P.: Problemes de matemàtica discreta. Universitat Jaume I, 1997

[Gall] Gallier, J.: Discrete Mathematics. Springer, 2011

[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3. ed. McGraw Hill, 2007

[Pla] Pla i Carrera, J.: Introducció a la metodologia de la Matemàtica. Universitat de Barcelona, 2006

[SchWie] Schafmeister, O., Wiebe, H.: Grundzüge der Algebra. B.G. Teubner, 1978

[StW] Storch, U. und Wiebe, H.: Lehrbuch der Mathematik, Band 2. Spektrum, Heidelberg, 1999

[Wall2] Wallis, W.D.: A beginner's guide to discrete mathematics. Second edition. Birkhäuser, 2012

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Capítulo 6. Aplicaciones

Durante buena parte de la matemática preuniversitaria y en asignaturas previas del Grado, como en Álgebra lineal o Cálculo, se habla continuamente de *aplicaciones lineales* y de *funciones*. De esta forma, ya se han visto ejemplos de un objeto matemático ubicuo cuya definición y propiedades generales son el objetivo de este capítulo; se basa en el concepto de correspondencia visto en el capítulo 4:

Definición. Una correspondencia $R \subseteq A \times B$ se llama *aplicación* si verifica las dos propiedades siguientes:

(a) $\mathrm{Dom}(R) = A$;
(b) $(a,b) \in R \wedge (a,c) \in R \implies b = c$.

Las aplicaciones son correspondencias, y por lo tanto se emplea toda la terminología de aquéllas. Normalmente las aplicaciones se denotan por letras minúsculas $f, g, h\ldots$ (a veces en el alfabeto griego φ, φ, $\psi\ldots$) y no por $R, S\ldots$ Además, se adopta la escritura $f : A \to B$ en vez de $R \subseteq A \times B$, y para denotar el hecho de que "a está relacionado con b por la relación (aplicación) f" se escribe $f(a) = b$ en vez de $a\ f\ b$ o $(a,b) \in f$, como es costumbre para relaciones en general.

Se puede tomar un punto de vista menos formalista, y sin considerar el concepto de correspondencia, se dice que una aplicación f de un conjunto A en un conjunto B es una regla que asigna a *cada* elemento de A *uno y solamente un* elemento de B; lo denotaremos de forma abreviada por

$$f : A \to B.$$

Al elemento del conjunto B al que se le asigna un elemento $x \in A$ vía f se le denota por $f(x)$, y recibe el nombre de *imagen* de x por f; el elemento x se llama *antiimagen*, *contraimagen* o *preimagen* de $f(x)$.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

No hemos hecho ninguna asunción sobre los conjuntos A y B, pero es fácil ver que si $A = \varnothing$, entonces existe exactamente una aplicación $\varphi : \varnothing \to B$ que llamamos aplicación vacía. En cambio, si $B = \varnothing$ y $A \neq \varnothing$, entonces no existe ninguna aplicación de A en B.

Observemos, por ejemplo, la figura siguiente:

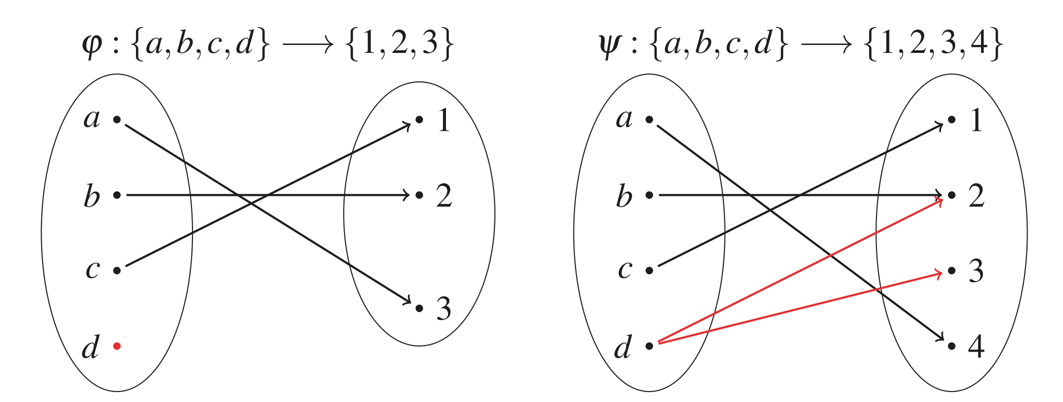


FIGURE 1. Ni φ ni ψ son aplicaciones.

El conjunto de partida de φ es el conjunto $A = \{a,b,c,d\}$, pero $\mathrm{Dom}(\varphi) = \{a,b,c\} \neq A$ (al elemento d no se le hace corresponder ningún elemento, luego φ no es una aplicación —se incumple la primera propiedad de la definición). En el caso de ψ, tiene dominio $\{a,b,c,d\}$, pero al elemento d se le hace corresponder más de un elemento —de hecho, dos— de su conjunto de llegada, por lo que tampoco es aplicación (no respeta la segunda propiedad de la definición).

Ejemplos. (i) Denotemos $\mathbb{R}_{\leq 0} := \{x \in \mathbb{R} : x \leq 0\}$. La correspondencia dada por

$$\begin{array}{rccc} f: & \mathbb{R} & \to & \mathbb{R}_{\leq 0} \\ & x & \mapsto & x^2 \end{array}$$

no es una aplicación: aunque la imagen de 0 es $0^2 = 0 \in \mathbb{R}_{\leq 0}$, el resto de elementos en $\mathbb{R}$ no se corresponden con elementos de $\mathbb{R}_{\leq 0}$ porque el cuadrado de un número real no nulo es siempre positivo, y el dominio de llegada está formado por números negativos o cero.

(ii) Denotemos $\mathbb{R}_{\geq 0} := \{x \in \mathbb{R} : x \geq 0\}$. La asignación dada por

$$f : \mathbb{R}_{\geq 0} \to \mathbb{R}, \quad f(x) = \pm\sqrt{x}$$

tampoco define una aplicación, pues todo elemento no nulo de $\mathbb{R}$ posee dos imágenes.

(iii) Las aplicaciones son conocidas desde la escuela, bajo la denominación de funciones, como por ejemplo

$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = x^2 \quad \text{para todo } x \in \mathbb{R}.$$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

(iv) Sobre cualquier conjunto $M \neq \varnothing$ se define la *aplicación identidad* (por abuso del lenguaje a menudo solamente llamada *la identidad*)

$$\mathrm{id}_M : M \to M, \quad \mathrm{id}_M(x) = x \quad \text{para todo } x \in M.$$

Dos aplicaciones $f : A \to B$, $g : C \to D$ coinciden si su dominio, su conjunto de llegada y la regla de asignación coinciden, es decir, si $A = C$, $B = D$ y $f(x) = g(x)$ para todo $x \in A$.

Sea $f : A \to B$ una aplicación. Para un subconjunto $A' \subseteq A$ definimos

$$f(A') := \{f(x) : x \in A'\};$$

$f(A')$ se denomina la *imagen* de A' por f. En el caso $A' = A$, en lugar de $f(A)$ escribiremos también Im f. Se puede comprobar que $A' = \varnothing$ si y solamente si $f(A') = \varnothing$. Además, para $A', A'' \subseteq A$ se demuestra que:

$$f(A' \cup A'') = f(A') \cup f(A'') \text{ y } f(A' \cap A'') \subseteq f(A') \cap f(A'').$$

Para $B' \subseteq B$ se define la *preimagen* (o contraimagen) de B' por f como

$$f^{-1}(B') := \{x \in A : f(x) \in B'\}.$$

En particular, para un elemento $y \in B$ se tiene

$$f^{-1}(y) := f^{-1}(\{y\}) = \{x \in A : f(x) = y\}.$$

Si $B', B'' \subseteq B$ y $A' \subseteq A$ se demuestra que:

$f^{-1}(f(A')) \supseteq A'$ y $f(f^{-1}(B')) \subseteq B'$;
$f^{-1}(B' \cup B'') = f^{-1}(B') \cup f^{-1}(B'')$ y $f^{-1}(B' \cap B'') = f^{-1}(B') \cap f^{-1}(B'')$.

Tomando como ejemplo la aplicación $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ se tiene

$$\begin{aligned} f(\mathbb{R}) = \mathrm{Im}(f) &= \{x \in \mathbb{R} : x \geq 0\}, \\ f(\{1,2,3\}) &= \{1,4,9\}, \\ f^{-1}(\{4\}) &= \{2,-2\}, \\ f^{-1}(\{-3\}) &= \varnothing, \\ f^{-1}(\{1,4,9\}) &= \{1,-1,2,-2,3,-3\}. \end{aligned}$$

A veces es importante restringir el conjunto imagen de una aplicación. Para una aplicación $f : A \to B$ y un subconjunto $A' \subseteq A$, la aplicación

$$f \mid A' : A' \to B$$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

definida por $(f \mid A')(x) = f(x)$ para todo $x \in A'$ recibe el nombre de *restricción* de f a A'. Cuando restringimos f al subconjunto A' lo único que estamos haciendo es aplicar la asignación dada por f solamente a los elementos de A'.

Definición. Sea $f : A \to B$ una aplicación.

(a) f es *inyectiva*, si para $x, x' \in A$ con $x \neq x'$ se tiene también $f(x) \neq f(x')$.
(b) f es *sobreyectiva*, si para cualquier $y \in B$ existe $x \in A$ tal que $f(x) = y$, es decir, si $\mathrm{Im}(f) = B$.
(c) f es *biyectiva*, si f es tanto inyectiva como sobreyectiva.

Nótese que la inyectividad se puede definir de manera equivalente como: una aplicación f es inyectiva si para $x, x' \in A$, de la igualdad $f(x) = f(x')$ se deduce la igualdad $x = x'$.

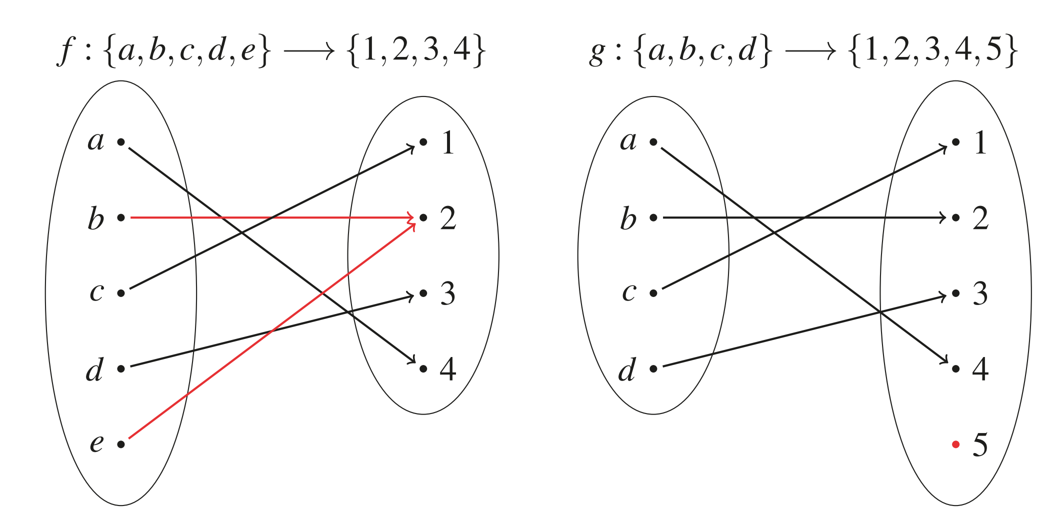


FIGURE 2. La aplicación f no es inyectiva, g no es sobreyectiva.

Ejemplos. (1) La aplicación identidad es obviamente biyectiva.
(2) Sea $\mathbb{R}_{\geq 0} = \{x \in \mathbb{R} : x \geq 0\}$. Definimos las aplicaciones

$$f_1 : \mathbb{R} \to \mathbb{R}, \quad f_2 : \mathbb{R}_{\geq 0} \to \mathbb{R}, \quad f_3 : \mathbb{R} \to \mathbb{R}_{\geq 0}, \quad f_4 : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$$

correspondiendo todas a la regla $f_i(x) = x^2$, $i = 1, \ldots, 4$. Entonces se verifica:

f_1 no es ni inyectiva ni sobreyectiva,
f_2 es inyectiva, pero no sobreyectiva,
f_3 no es inyectiva, pero es sobreyectiva,
f_4 es biyectiva.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Veamos que f_1 no es inyectiva: para ello basta observar que existen al menos dos elementos distintos con la misma imagen; efectivamente 1 y -1, por ejemplo, verifican lo requerido, pues son distintos pero $f_1(1) = f_1(-1) = 1$.

Veamos que f_1 no es sobreyectiva. Es suficiente encontrar al menos un elemento en el espacio de llegada $\mathbb{R}$ que no pertenece a $\mathrm{Im}(f_1)$, es decir, que no posee contraimagen; esto lo verifica cualquier número real negativo, por ejemplo -1: $-1 \in \mathbb{R}$ pero $-1 \notin \mathrm{Im}(f_1)$, porque no existen ningún número real que al aplicarlo f_1, esto es, elevarlo a cuadrado, dé -1.

Veamos que f_2 es inyectiva. Sean para ello $x, y \in \mathbb{R}_{\geq 0}$ (es decir, no negativos). En principio se tiene que

$$f_2(x) = f_2(y) \Longleftrightarrow x^2 = y^2 \Longrightarrow x = \pm y,$$

pero como ni x ni y son negativos, lo que en realidad se deduce de la igualdad $x^2 = y^2$ es $x = y$, lo que prueba la inyectividad de f_2.

Veamos para terminar que f_3 es sobreyectiva. Consideremos para ello $z \in \mathbb{R}_{\geq 0}$ arbitrario. Si encontramos un $x \in \mathbb{R}$ tal que $f_3(x) = z$ hemos terminado. Pero como z no es negativo, podemos tomar $\sqrt{z} \in \mathbb{R}$, y este es exactamente el x buscado: efectivamente, haciendo $x := \sqrt{z}$ se cumple lo requerido:

$$f_3(x) = x^2 = (\sqrt{z})^2 = z.$$

La substitución de x por $\sqrt{z}$ y su posterior elevación al cuadrado del ejemplo anterior sugiere la idea de que las funciones se pueden concatenar: hemos aplicado la función "substituir x por raíz cuadrada de z" primero, para después aplicar sobre el resultado una segunda función "elevar al cuadrado". Es un principio general:

Definición. Sean las aplicaciones $f : A \to B$ y $g : B \to C$. La aplicación

$$g \circ f : A \to C, \quad (g \circ f)(x) = g(f(x))$$

se llama *composición* (también: concatenación) de f con g.

De manera algo más precisa se puede decir que la composición $g \circ f$ de una aplicación $f : A \to B'$ con una aplicación $g : B \to C$ está bien definida siempre que $\mathrm{Im} f \subseteq B$. La composición de aplicaciones es un caso particular de la composición de correspondencias vista en el capítulo 4.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Por **ejemplo**, para las aplicaciones $f, g : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ y $g(y) = 3 + y$, se tiene

$$(g \circ f)(x) = g(f(x)) = g(x^2) = 3 + x^2,$$
$$(f \circ g)(x) = f(g(x)) = f(3 + x) = (3 + x)^2.$$

Este ejemplo muestra, en particular, cuán lejos está la operación $\circ$ entre aplicaciones de ser "conmutativa": ¡el orden a la hora de componer aplicaciones importa!

Una vez conocida la composición de aplicaciones podemos dar una caracterización de las aplicaciones biyectivas, que al mismo tiempo resuelve el problema de la "reversibilidad" de una aplicación, esto es, bajo qué condiciones se puede deducir de una aplicación $A \to B$ otra $B \to A$:

Teorema y definición 6.1. *Sean A,B dos conjuntos no vacíos. Una aplicación $f : A \to B$ es biyectiva si y sólo si existe una aplicación $g : B \to A$ tal que*

$$f \circ g = id_B \;\text{ y }\; g \circ f = id_A,$$

donde id_B resp. id_A es la identidad en B resp. la identidad en A. En este caso la aplicación g está unívocamente determinada por f, y se denota por f^{-1}. La aplicación f^{-1} se llama la aplicación inversa *o recíproca de f.*

Demostración. Este teorema tiene dos partes, una de existencia de la función g y otra de su unicidad.
Existencia:
Supongamos primero que f sea una biyección. Para cada $y \in B$ existe entonces un único $x_y \in A$ con $f(x_y) = y$. Se define la aplicación $g : B \to A$ como $g(y) = x_y$. Por una parte se tiene

$$(f \circ g)(y) = f(g(y)) = f(x_y) = y = id_B(y)$$

y así $f \circ g = id_B$. Por otra parte, para cualquier $x \in A$, por las definiciones de "$\circ$" y de g es claro que

$$(g \circ f)(x) = g(f(x)) = x,$$

de donde $g \circ f = id_A$. Recíprocamente, consideremos la aplicación $g : B \to A$ tal que $f \circ g = id_B$ y $g \circ f = id_A$. Sea $y \in B$, para $x := g(y) \in A$ se verifica que

$$y = id_B(y) = (f \circ g)(y) = f(g(y)) = f(x),$$

luego f es sobreyectiva. Si vemos que f es inyectiva habremos terminado. Sean para ello $x, x' \in A$ tales que $f(x) = f(x')$; entonces

$$x = id_A(x) = (g \circ f)(x) = g(f(x)) = g(f(x')) = (g \circ f)(x') = id_A(x') = x',$$

lo que prueba la inyectividad de f.
Unicidad:
Supongamos que junto a $g : B \to A$ con las condiciones del enunciado existiera otra

aplicación $h : B \to A$ tal que $f \circ h = id_B$ y $h \circ f = id_A$; veamos que ha de coincidir con g: para ello, tomando cualquier $y \in B$ se tiene que

$$g(y) = g(\mathrm{id}_B(y)) = g(f(h(y))) = (g \circ f)(h(y)) = \mathrm{id}_A(h(y)) = h(y),$$

lo que prueba la unicidad. □

¡Atención! Tanto la aplicación inversa de f —caso de existir— como el conjunto preimagen de f —que existe siempre— se denotan por el mismo símbolo f^{-1}. Dado el caso se distinguirá una situación de la otra según el contexto. Tal notación está tan fuertemente establecida que no podemos renunciar a ella.

En virtud del Teorema 6.1, una aplicación biyectiva $f : A \to B$ hace posible la transferencia de datos sobre A a datos sobre B de manera unívoca; la aplicación inversa describe la transferencia en el sentido contrario, de B a A.

¿Qué es contar? Este capítulo pone de manifiesto que muchos procesos en matemáticas se pueden describir de forma precisa recurriendo a las aplicaciones. Un ejemplo es el hecho de contar los elementos de un conjunto. Empecemos definiendo: dos conjuntos A y B se dicen *equipotentes* si se puede encontrar una biyección $f : A \to B$. Un conjunto M se dice finito si es equipotente a un conjunto del tipo $\{1, 2, \ldots, n\}$, y de lo contrario se dice infinito; se llama infinito numerable si es equipotente a $\mathbb{N}$, y se llama numerable si es finito o infinito numerable. Si no se puede establecer biyección alguna entre M y $\mathbb{N}$ se dice que M es *infinito no numerable*.

Hay fenómenos sorprendentes en esta teoría de cardinales: se puede probar, por ejemplo, que cualquier subconjunto propio de $\mathbb{N}$ infinito es equipotente a $\mathbb{N}$. Además, $\mathbb{Q}$ es equipotente a $\mathbb{N}$ (¿por qué?). Otro resultado importante es el que afirma que la potencia de un conjunto infinito es "mayor" que el conjunto mismo (para conjuntos finitos ya lo hemos probado, ver Teorema 3.1):

Teorema 6.2 (Teorema de Cantor)**.** *Sea M un conjunto, entonces el conjunto potencia $\mathscr{P}(M)$ no es equipotente a M.*

Demostración. Razonemos por reducción al absurdo y supongamos que existiera una aplicación sobreyectiva $f : M \to \mathscr{P}(M)$. Definamos el conjunto

$$N := \{x \in M : x \notin f(x)\}$$

(fijémonos en que x es un elemento de M, pero $f(x)$ es un subconjunto de M). Como f es sobreyectiva, existirá $y \in M$ tal que $f(y) = N \in \mathscr{P}(M)$. Ahora bien, pueden pasar dos casos:

(i) $y \in N$, luego $y \notin f(y)$, luego $y \notin N$, absurdo;

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

(ii) $y \in M \setminus N$, luego $y \in f(y)$, luego $y \in N$, absurdo;
es decir, y no es elemento ni de N ni de $M \setminus N$, lo cual es imposible. Por lo tanto no puede existir ninguna aplicación sobreyectiva de M en $\mathscr{P}(M)$, en particular ninguna biyectiva. $\square$

Este teorema el punto de partida de la teoría de cardinales: efectivamente el conjunto $\mathscr{P}(\mathbb{N})$ posee un cardinal mayor —en el sentido expuesto— que $\mathbb{N}$, pero por lo mismo el conjunto $\mathscr{P}(\mathscr{P}(\mathbb{N}))$ posee un cardinal mayor que $\mathscr{P}(\mathbb{N})$, y así *ad nauseam*. Es decir, existen "infinitos" infinitos (¡!) de diferentes tamaños. En la colección de todos ellos se sabe ubicar a $\mathbb{R}$: es equipotente a $\mathscr{P}(\mathbb{N})$. Una demostración se debe al mismo Cantor, pero no la vamos a tratar en este curso. (¡Es un buen ejercicio!)

Un resultado también importante dentro de esta teoría, que enunciamos sin demostración, es:

Teorema 6.3 (Teorema de Schröder-Bernstein[1]). *Sean A y B dos conjuntos. Si existen aplicaciones inyectivas $f : A \to B$ y $g : B \to A$, entonces existe una aplicación biyectiva $h : A \to B$ (es decir, A y B son equipotentes).*

El Teorema de Schröder-Bernstein es un resultado muy básico en el orden lógico; se puede probar que es equivalente al axioma de elección, que es uno de los que componen la axiomática de Zermelo-Fraenkel que comentamos al final del capítulo 3.

[1]Por los alemanes Ernst SCHRÖDER (1841–1902) y Felix BERNSTEIN (1878–1956).

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

[Ant] Antoine, R., Camps, R., Moncasi, J.: Introducció a l'àlgebra abstracta. Universitat Autònoma de Barcelona, 2007

[Big] Biggs, N.L.: Discrete Mathematics. Second ed. Oxford U.P., 2004

[Conr] Conradie, W., Goranko, V.: Logic and Discrete Mathematics. A concise introduction. Wiley, 2015

[FG] Ferrando, J.C., Gregori, V.: Matemática Discreta. 2. ed. Reverté, 2002

[GOV] Galindo Pastor, C., Orús Báguena, M.P., Vindel Cañas, M.P.: Problemes de matemàtica discreta. Universitat Jaume I, 1997

[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3. ed. McGraw Hill, 2007

[Pla] Pla i Carrera, J.: Introducció a la metodologia de la Matemàtica. Universitat de Barcelona, 2006

[SchWie] Schafmeister, O., Wiebe, H.: Grundzüge der Algebra. B.G. Teubner, 1978

[Wall2] Wallis, W.D.: A beginner's guide to discrete mathematics. Second edition. Birkhäuser, 2012

Capítulo 7. Álgebras de Boole

Consideremos un conjunto M y su conjunto potencia, es decir, el conjunto de todos los subconjuntos $N \subseteq M$. Si consideramos las operaciones unión "$\cup$", intersección "$\cap$" y el complemento "$\bar{\ }$" de conjuntos, es fácil comprobar que, para cualesquiera $A,B,C \subseteq M$, se verifican las cuatro propiedades dobles siguientes:

(a) $A \cup B = B \cup A$ y $A \cap B = B \cap A$;
(b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ y $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
(c) $A \cup \emptyset = A$ y $A \cap M = A$;
(d) $A \cup \bar{A} = M$ y $A \cap \bar{A} = \emptyset$.

(¡La demostración cuidadosa de estas propiedades es un buen ejercicio!)

Este patrón de propiedades se repite en otros rincones de las matemáticas, por lo que merece la pena abstraerlas en un contexto general.

Precisamente el presente capítulo se dedica a una introducción al estudio de este contexto: un conjunto (que jugará el papel de M) con tres operaciones (que tomarán los roles de la intersección, la unión y el complemento) que cumplen las cuatro propiedades dobles anteriores se denomina *álgebra de Boole*[1]. Las proposiciones propias de estos espacios se llaman expresiones booleanas, y son de capital importancia en informática.

Comencemos, pues, abstrayendo las operaciones con las que se definirá una álgebra de Boole.

Una *operación binaria* sobre un conjunto S (también llamada ley de composición interna sobre S) es un modo de combinar dos elementos cualesquiera del conjunto de forma que se les asocie unívocamente (es decir, sin equívocos) un elemento de S; en otras palabras, se trata de una *aplicación* $S \times S \to S$.

[1]Honrando la memoria del matemático y lógico británico George BOOLE (1815–1864).

Por ejemplo, la suma de dos números naturales cualesquiera es de nuevo un número natural (¡y sólo uno!). Sin embargo, no ocurre lo mismo con la resta: $2-3=-1\notin\mathbb{N}$. La suma de números naturales es una operación binaria sobre $\mathbb{N}$, no así la resta.

También hay operaciones *monarias*, que solamente afectan a un elemento de la colección: piénsese por ejemplo en la operación "elevar al cuadrado", o "tomar el inverso de un número real no nulo".

Tómese un conjunto B con dos elementos distinguidos, denotados por "0" y por "1". Supóngase que sobre B están definidas dos operaciones binarias, denotadas[2] por "$+$" y por "$\cdot$", y una operación monaria, denotada por " $^{-}$ "; escríbase $x+y$ resp. $x\cdot y$ al resultado de aplicar la operación "$+$" resp. "$\cdot$" a los elementos x,y de B, y $\bar{x}$ al de aplicar la operación monaria a un elemento $x\in B$.

Se dice entonces que B, junto con las dos operaciones binarias y la monaria anteriores, posee estructura de *álgebra de Boole* si *para cualesquiera* elementos $x,y,z\in B$ se verifican las propiedades siguientes:

(B1) Leyes conmutativas:

$$\text{(a)}\quad x+y=y+x$$
$$\text{(b)}\quad x\cdot y=y\cdot x$$

(B2) Leyes distributivas

$$\text{(a)}\quad x+(y\cdot z)=(x+y)\cdot(x+z)$$
$$\text{(b)}\quad x\cdot(y+z)=x\cdot y+x\cdot z$$

(B3) Leyes de identidad

$$\text{(a)}\quad x+0=x$$
$$\text{(b)}\quad x\cdot 1=x$$

(B4) Leyes de complemento

$$\text{(a)}\quad x+\bar{x}=1$$
$$\text{(b)}\quad x\cdot\bar{x}=0$$

Estas propiedades (B1)–(B4) se llaman *axiomas de álgebra de Boole*.

[2] Aunque usamos los signos familiares "+" y "·", su significado nada tiene que ver en principio con los "+" y "·" usuales; bien podríamos haber usado otros símbolos, como por ejemplo "$\vee$" resp. "$\wedge$".

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Nota. (1) Los elementos "0" y "1" reciben el nombre de "cero" y "unidad" del álgebra de Boole. Además, se suele escribir $(B, +, \cdot, ^{-}, 0, 1)$ si se desea remarcar las operaciones y elementos distinguidos del álgebra de Boole B.

(2) Las operaciones "+" y "·" se suelen denominar "suma" y "producto" del álgebra de Boole, pero no deben confundirse con la suma y productos de la aritmética usual; en ella, la propiedad (B2)(a), por ejemplo, no se verifica:

$$1 = 1 + (2 \cdot 0) \neq (1 + 2) \cdot (1 + 0) = 3.$$

(3) El elemento $\bar{x}$ se llama *complemento* de x.

Ejemplos. (1) El primer ejemplo es el de partida: dado un conjunto, su conjunto potencia junto con las operaciones unión "$\cup$", intersección "$\cap$" y complemento "$^{-}$" de conjuntos posee estructura de álgebra de Boole.

(2) Retomemos el ejemplo (2) del capítulo 5 y sea $\mathfrak{P}$ el conjunto de las proposiciones simples. Vimos que la relación "ser lógicamente equivalente"

$$p \equiv q \;:\Longleftrightarrow\; p \Leftrightarrow q, \quad p, q \in \mathfrak{P}$$

es de equivalencia. Si denotamos por P al conjunto cociente,

$$P := \mathfrak{P}/\equiv,$$

entonces P junto a las operaciones disyunción "$\vee$", que juega el papel de la suma "+", conjunción "$\wedge$", que juega el papel del producto "·", y negación "$\neg$", que asume el papel del complemento, posee estructura de álgebra de Boole: ver que se verifican los axiomas (B1)–(B4) es muy sencillo con ayuda de las tablas de verdad. Nótese que el elemento "0" representa las contradicciones y el "1" las tautologías.

(3) Sea $\mathbb{B} := \{0, 1\}$; definamos una suma, un producto y un complemento sobre $\mathbb{B}$ de acuerdo a las tablas siguientes:

+	0	1
0	0	1
1	1	1

·	0	1
0	0	0
1	0	1

x	$\bar{x}$
0	1
1	0

Es fácil comprobar que $\mathbb{B}$ posee, respecto de estas operaciones, estructura de álgebra de Boole.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

(4) El producto cartesiano $B_1 \times \cdots \times B_n$ de n álgebras de Boole $B_1, \dots, B_n$ es una álgebra de Boole (para verlo basta trabajar componente a componente). En particular, $\mathbb{B}^n$ tiene estructura de álgebra de Boole cuando se aplican las operaciones de (3) componente a componente.

Convenciones. (1) Adoptaremos las siguientes reglas de precedencia para las operaciones:

$$\text{“}\,^{-}\,\text{”} \quad \text{precede a} \quad \text{“}\cdot\text{”}, \quad \text{que precede a} \quad \text{“}+\text{”}.$$

Por ejemplo, la expresión $x + y \cdot z$ quiere decir $x + (y \cdot z)$ y no $(x + y) \cdot z$.

(2) Se omitirá, por regla general, el signo “$\cdot$” del producto: así, escribiremos xy y no $x \cdot y$, o bien $(x+z)(x+y)$ y no $(x+z)\cdot(x+y)$, a no ser que razones de legibilidad de escritura lo aconsejaren, como en $x \cdot 0 = 0$.

A la vista de los axiomas (B1) a (B4) de álgebra de Boole, se aprecia que para cada uno de ellos aparecen dos formulaciones, (a) y (b), en las que se han cambiado 0 por 1 y adición por producto. La generalización de este hecho para cualquier *expresión booleana*[3], es decir, para una expresión construida a partir de las variables usando “$+$”, “$\cdot$” y “$\,^{-}\,$”, además de paréntesis, se denomina *dualidad*.

Ejemplo. Sea B una álgebra de Boole. Sean x, y, z elementos de B. Las expresiones $x + y + z$, $\bar{y}$, $xzy + \bar{y}$, $(x+y)(x+\bar{y})\dots$ son ejemplos de expresiones booleanas. La igualdad

$$(1 + x)(y + 0) = y$$

es otro ejemplo de expresión booleana, cuyo dual es

$$(0 \cdot x) + (y \cdot 1) = y.$$

En particular, los axiomas de álgebra de Boole son invariantes por dualidad, de lo que se deduce:

Teorema 7.1 (Principio de dualidad)**.** *Sea B una álgebra de Boole. El dual de un teorema en B es un teorema en B.*

El principio de dualidad permite simplificar muchas demostraciones. Veamos su utilidad al tiempo que introducimos algunas reglas operativas típicas de las expresiones booleanas.

[3] La noción de expresión booleana cobrará significado propio en el capítulo siguiente.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Teorema 7.2. *Sea B una álgebra de Boole. Para cualesquiera x,y,z elementos de B se verifican las propiedades siguientes:*

(B5) *Leyes de idempotencia:*

$$\text{(a)}\ \ x+x=x$$
$$\text{(b)}\ \ xx=x$$

(B6) *Leyes de acotación:*

$$\text{(a)}\ \ x+1=1$$
$$\text{(b)}\ \ x\cdot 0=0$$

(B7) *Leyes de absorción:*

$$\text{(a)}\ \ x+(xy)=x$$
$$\text{(b)}\ \ x(x+y)=x$$

(B8) *Leyes asociativas:*

$$\text{(a)}\ \ x+(y+z)=(x+y)+z$$
$$\text{(b)}\ \ x(yz)=(xy)z$$

Demostración. Basta con demostrar por ejemplo las partes (b) de las leyes, pues las partes (a) se siguen aplicando el principio de dualidad (Teorema 7.1). Así, la segunda ley de idempotencia se deduce de la aplicación sucesiva de las leyes de identidad, complemento, distributiva, y de nuevo complemento e identidad:

$$xx \overset{(B3)}{=} (xx)+0 \overset{(B4)}{=} (xx)+(x\bar{x}) \overset{(B2)}{=} x(x+\bar{x}) \overset{(B4)}{=} x\cdot 1 \overset{(B3)}{=} x.$$

La segunda ley de acotación hace, además, uso de las leyes conmutativas:

$$x\cdot 0 \overset{(B3)}{=} (x\cdot 0)+0 \overset{(B4)}{=} (x\cdot 0)+(x\bar{x}) \overset{(B2)}{=} x(0+\bar{x}) \overset{(B1)}{=} x(\bar{x}+0) \overset{(B3)}{=} x\bar{x} \overset{(B4)}{=} 0.$$

La segunda ley de absorción aprovecha la segunda ley de acotación recién demostrada:

$$x(x+y) \overset{(B3)}{=} (x+0)(x+y) \overset{(B2)}{=} x+(0\cdot y) \overset{(B1)}{=} x+(y\cdot 0) \overset{(B6)}{=} x+0 \overset{(B3)}{=} x.$$

La prueba de leyes asociativas es algo más complicada: denotemos $L := (xy)z$ y $R := x(yz)$. Queremos demostrar $L=R$. Probemos primero que $x+L=x+R$. Lo hacemos en dos pasos:
(i) $x+L=x$, ya que:

$$x+L=x+((xy)z) \overset{(B2)}{=} (x+(xy))(x+z) \overset{(B7)}{=} x(x+z) \overset{(B7)}{=} x;$$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

(ii) $x+R=x$, pues

$$x+R = x+(x(yz)) \overset{(B2)}{=} (x+x)(x+(yz)) \overset{(B5)}{=} x(x+(yz)) \overset{(B7)}{=} x.$$

Además se verifica que $\bar{x}+L=\bar{x}+R$, ya que, por una parte

$$\begin{aligned}\bar{x}+L = \bar{x}+((xy)z) &\overset{(B2)}{=} (\bar{x}+(xy))(\bar{x}+z)\\ &\overset{(B2)}{=} ((\bar{x}+x)(\bar{x}+y))(\bar{x}+z) \overset{(B4)}{=} (1\cdot(\bar{x}+y))(\bar{x}+z)\\ &\overset{(B3)}{=} (\bar{x}+y)(\bar{x}+z) \overset{(B2)}{=} \bar{x}+(yz),\end{aligned}$$

y por otra parte

$$\begin{aligned}\bar{x}+R = \bar{x}+(x(yz)) &\overset{(B2)}{=} (\bar{x}+x)(\bar{x}+(yz))\\ &\overset{(B4)}{=} 1\cdot(\bar{x}+(yz)) \overset{(B3)}{=} \bar{x}+(yz).\end{aligned}$$

Por lo tanto $\bar{x}+R=\bar{x}+L$, y junto con lo anterior se deduce la igualdad de L y R:

$$\begin{aligned}L &\overset{(B3)}{=} 0+L \overset{(B4)}{=} (x\bar{x})+L\\ &\overset{(B2)}{=} (x+L)(\bar{x}+L) = (x+R)(\bar{x}+R)\\ &\overset{(B2)}{=} (x\bar{x})+R \overset{(B4)}{=} 0+R \overset{(B3)}{=} R.\end{aligned}$$

□

Teorema 7.3. *Sea B una álgebra de Boole. Se verifican los asertos siguientes:*

(1) *Unicidad del complemento: Para $x\in B$, si $x+z \overset{(*)}{=} 1$ y $xz \overset{(**)}{=} 0$, entonces $z=\bar{x}$ para todo $z\in B$.*
(2) *Ley de involución: para cualquier $x\in B$ se tiene que $\bar{\bar{x}}=x$.*
(3) *Se tiene que $\bar{0}=1$ y $\bar{1}=0$.*

Demostración. (1) Por una parte se tiene que

$$\bar{x} \overset{(B3)}{=} \bar{x}+0 \overset{(**)}{=} \bar{x}+(xz) \overset{(B2)}{=} (\bar{x}+x)(\bar{x}+z) \overset{(B4)}{=} 1\cdot(\bar{x}+z) \overset{(B3)}{=} \bar{x}+z.$$

Por otra parte se cumple

$$z \overset{(B3)}{=} z+0 \overset{(B4)}{=} z+(x\bar{x}) \overset{(B2)}{=} (z+x)(z+\bar{x}) \overset{(*)}{=} 1\cdot(z+\bar{x}) \overset{(B3)}{=} z+\bar{x}.$$

Entonces se verifica

$$z = z+\bar{x} \overset{(B1)}{=} \bar{x}+z = \bar{x},$$

como se quería.

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

(2) Por las leyes de complemento (B4) se tiene $x+\bar{x}=1, x\bar{x}=0$; aplicando las leyes conmutativas (B1) se verifica entonces que $\bar{x}+x=1, \bar{x}x=0$. Por lo tanto, por la unicidad del complemento (1) se colige que x ha de ser el complemento de $\bar{x}$, es decir, que $\bar{\bar{x}}=x$.

(3) Del aserto (B6)(a) en el Teorema 7.2 se deduce que $0+1=1$, y por el axioma de identidad (B3)(b) es $0\cdot 1=0$. La unicidad del complemento permite concluir que $1=\bar{0}$. El principio de dualidad nos ofrece además que $0=\bar{1}$. □

Teorema 7.4. *(Leyes de* de Morgan*).*[4] *Sea B una álgebra de Boole y consideremos $x, y \in B$. Se cumple:*

$$\begin{array}{rrcl} \text{(a)} & \overline{x+y} & = & \bar{x}\cdot\bar{y} \\ \text{(b)} & \overline{x\cdot y} & = & \bar{x}+\bar{y} \end{array}$$

Demostración. Vamos a probar (a), y (b) se deduce inmediatamente por el principio de dualidad. Para demostrar (a), basta ver que se verifican

$$(x+y)+(\bar{x}\bar{y})=1 \;\text{ y }\; (x+y)(\bar{x}\bar{y})=0,$$

pues en tal caso la unicidad del complemento nos permite concluir que

$$\bar{x}\bar{y}=\overline{x+y}.$$

La primera igualdad se satisface:

$$\begin{aligned}(x+y)+(\bar{x}\bar{y}) &\overset{(B1)}{=} (y+x)+(\bar{x}\bar{y}) \overset{(B8)}{=} y+(x+\bar{x}\bar{y}) \\ &\overset{(B2)}{=} y+((x+\bar{x})(x+\bar{y})) \overset{(B4)}{=} y+(1\cdot(x+\bar{y})) \\ &\overset{(B3)}{=} y+(x+\bar{y}) \overset{(B1)}{=} y+(\bar{y}+x) \overset{(B8)}{=} (y+\bar{y})+x \overset{(B4)}{=} 1+x \\ &\overset{(B6)}{=} 1.\end{aligned}$$

Análogamente se verifica la segunda igualdad:

$$\begin{aligned}(x+y)(\bar{x}\bar{y}) &\overset{(B8)}{=} ((x+y)\bar{x})\bar{y} \overset{(B2)}{=} ((x\bar{x})+(y\bar{x}))\bar{y} \\ &\overset{(B4)}{=} (0+(y\bar{x}))\bar{y} \overset{(B3)}{=} (y\bar{x})\bar{y} \\ &\overset{(B1)}{=} \bar{y}(y\bar{x}) \overset{(B8)}{=} (\bar{y}y)\bar{x} \overset{(B4)}{=} 0\cdot\bar{x} \\ &\overset{(B6)}{=} 0.\end{aligned}$$

La aplicación del Teorema 7.3 (1) (unicidad del complemento) permite concluir. □

[4] Por el matemático británico Augustus De Morgan (1806–1871).

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Terminamos el capítulo presentando las aplicaciones que son genuinas para las álgebras de Boole: los homomorfismos de álgebras de Boole.

Definición. Sean $B_1 = (B_1, +_1, \cdot_1, ^{-1}, 0_1, 1_1)$ y $B_2 = (B_2, +_2, \cdot_2, ^{-2}, 0_2, 1_2)$ dos álgebras de Boole. Una aplicación $f : B_1 \to B_2$ se dice que es un *homomorfismo* de álgebras de Boole si para cualesquiera $x, y \in B_1$ se verifica:

(HB1) $f(x +_1 y) = f(x) +_2 f(y)$;
(HB2) $f(x \cdot_1 y) = f(x) \cdot_2 f(y)$;
(HB3) $f(\overline{x}^1) = \overline{f(x)}^2$.

Un *isomorfismo* de álgebras de Boole es un homomorfismo de álgebras de Boole biyectivo tal que su inversa es también un homomorfismo de álgebras de Boole.

La demostración de las siguientes observaciones es un buen ejercicio:

(a) La definición de homomorfismo de álgebras de Boole que hemos dado es redundante: basta exigir los axiomas (HB1) y (HB3) o los axiomas (HB2) y (HB3); es decir
$$\big[\text{(HB1)} \wedge \text{(HB3)} \implies \text{(HB2)}\big] \ \vee \ \big[\text{(HB2)} \wedge \text{(HB3)} \implies \text{(HB1)}\big].$$
(b) Para un homomorfismo $f : B_1 \to B_2$ de álgebras de Boole se verifica que $f(0_1) = 0_2$ y $f(1_1) = 1_2$.
(c) La definición de isomorfismo presentada también es redundante en el sentido siguiente: si $f : B_1 \to B_2$ es un homomorfismo biyectivo de álgebras de Boole entonces es un isomorfismo, es decir, su inversa también es un homomorfismo.

Ejemplo. Sean $N \subseteq M$ dos conjuntos y sean sus conjuntos potencias $\mathscr{P}(N)$ y $\mathscr{P}(M)$. La aplicación $f : \mathscr{P}(M) \to \mathscr{P}(N)$ definida por $f(A) = A \cap N$ para cualquier $A \in \mathscr{P}(M)$ es un homomorfismo de álgebras de Boole.

En el capítulo siguiente aclararemos qué se entiende por "expresiones booleanas" y cómo se forman funciones a partir de ellas.

ISBN: 978-84-17900-65-6

DOI: http://dx.doi.org/10.6035/Sapientia170

[Conr] Conradie, W., Goranko, V.: Logic and Discrete Mathematics. A concise introduction. Wiley, 2015
[FG] Ferrando, J.C., Gregori, V.: Matemática Discreta. 2. ed. Reverté, 2002
[GOV] Galindo Pastor, C., Orús Báguena, M.P., Vindel Cañas, M.P.: Problemes de matemàtica discreta. Universitat Jaume I, 1997
[Gall] Gallier, J.: Discrete Mathematics. Springer, 2011
[Ham] Hamilton, A.G.: Logic for mathematicians, Cambridge U.P. 1978
[LiPi] Lidl, R., Pilz, G.: Applied Abstract Algebra. Second edition. Springer, 1998
[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3. ed. McGraw Hill, 2007
[Rios] Ríos, S.: Matemática finita. Paraninfo, 1974
[Smull] Smullyan, R.M.: A Beginner's guide to Mathematical Logic. Dover, 2014
[Wall2] Wallis, W.D.: A beginner's guide to discrete mathematics. Second edition. Birkhäuser, 2012

Capítulo 8. Polinomios y funciones booleanas

Sea $\{x_1, \dots, x_n\}$ un conjunto de símbolos (o indeterminadas) distintos de 0 y de 1. (Cuando solamente se precisan tres o menos símbolos se suele emplear x, y, z). Aunque ya hemos hablado de manera informal de expresiones booleanas en el capítulo previo, las presentamos aquí formalmente:

Definición. Un *polinomio booleano* en $\{x_1, \dots, x_n\}$ es una expresión formal que se puede construir en un número finito de pasos con las siguientes reglas:

(a) $0, 1, x_1, \dots, x_n$ son polinomios booleanos;
(b) si p y q son polinomios booleanos, también lo son

$$p + q, \ p \cdot q, \ \overline{p}.$$

Se admite además el uso de paréntesis para distinguir el orden de precedencia de las operaciones.

Los polinomios booleanos se denominan también “expresiones booleanas” en la literatura. Además, un polinomio booleano en $\{x_1, \dots, x_n\}$ se llama, sobreentendiendo el nombre de las indeterminadas, de n-ésimo orden (o de orden n). Al conjunto de polinomios booleanos de n-ésimo orden lo denotaremos por $\mathscr{P}_n$.

Ejemplos. Son polinomios booleanos, todos distintos entre sí, los siguientes:

$$0, \overline{0}, 1, x, 0 + x, y, z, (x + y) + z.$$

A los polinomios booleanos se les aplican las mismas convenciones que para las operaciones de las álgebras de Boole. Por ejemplo, $x + y + z$ y $x + y \cdot z$ son considerados idénticos a $(x + y) + z = x + (y + z)$ y $x + (y \cdot z)$, respectivamente. Es decir, escribiremos xy en lugar de $x \cdot y$, minimizaremos el uso de paréntesis, etc. Esto significa que la expresión $x + yz$ adquiere el mismo significado que $x + (yz)$ después de establecer el convenio, pero no antes. La expresión $x + y + z$ adquiere significado una vez verificada la validez de la propiedad asociativa para “+”, si es el caso (que lo es).

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Los polinomios booleanos pueden ser considerados aplicaciones sobre álgebras de Boole en el sentido siguiente:

Definición. Sea p un polinomio booleano en $\{x_1,\ldots,x_n\}$, y sea B una álgebra de Boole. Se denota por $\tilde{p}_B$ la aplicación

$$\begin{array}{cccc} \tilde{p}_B: & B^n & \longrightarrow & B \\ & (b_1,\ldots,b_n) & \longmapsto & p(b_1,\ldots,b_n) \end{array}$$

donde $p(b_1,\ldots,b_n)$ se forma substituyendo 0 por el 0 de B, 1 por el 1 de B, y x_i por b_i para todo $i=1,\ldots,n$, y operando en B. Así, $\tilde{p}_B$ se denomina *función booleana* de orden n sobre B (asociada a p). Si no hay riesgo de confusión escribiremos $\tilde{p}$ en vez de $\tilde{p}_B$.

Las funciones booleanas se pueden evaluar para valores conocidos:

Ejemplos. (a) Considérese el polinomio booleano $a = xy\bar{z}+x(y+z)$ en $\{x,y,z\}$. Podemos considerarlo como una función $\tilde{a}=\tilde{a}_{\mathbb{B}}:\mathbb{B}^3\to\mathbb{B}$, y por tanto, es posible evaluarlo para cualquier elemento de $\mathbb{B}^3$, por ejemplo en $(1,0,0)$:

$$\begin{aligned} \tilde{a}_{\mathbb{B}}(1,0,0) &= 1\cdot 0\cdot\bar{0}+1(0+0) \\ &= 1\cdot 0\cdot 1+1\cdot 0 = 1\cdot 0+1\cdot 0 \\ &= 0+0=0, \end{aligned}$$

usando solamente los axiomas de álgebra de Boole.

(b) Sea B una álgebra de Boole, y consideremos la función booleana

$$f: B^3\to B,\ f(x,z,y)=x+xy+\bar{y}z.$$

Entonces f es una función booleana de orden 3 sobre B. De hecho,

(i) si B es el álgebra de Boole definida por el conjunto potencia $\mathscr{P}(M)$ de un conjunto M, entonces

$$\tilde{f}_B(X,Y,Z)=X\cup(X\cap Y)\cup((M\setminus Y)\cap Z);$$

(ii) si B es el álgebra de Boole de las proposiciones, esta función f corresponde a la proposición

$$\tilde{f}_B(p,q,r)=p\vee(p\wedge q)\vee(\neg q\wedge r).$$

Polinomios booleanos distintos pueden dar lugar a la misma función booleana, como muestra el siguiente ejemplo sencillo:

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Ejemplo. En $\{x,y\}$ consideramos los polinomios booleanos $p = xy$ y $q = yx$, que son polinomios *distintos*. Sin embargo, sobre el álgebra de Boole $B := \mathbb{B} = \{0,1\}$ definen la misma función booleana:

$$\begin{array}{cccc} \tilde{p}_B : & B^n & \longrightarrow & B \\ & (0,0) & \longmapsto & 0 \cdot 0 = 0 \\ & (0,1) & \longmapsto & 0 \cdot 1 = 0 \\ & (1,0) & \longmapsto & 1 \cdot 0 = 0 \\ & (1,1) & \longmapsto & 1 \cdot 1 = 1 \end{array} \qquad \begin{array}{cccc} \tilde{q}_B : & B^n & \longrightarrow & B \\ & (0,0) & \longmapsto & 0 \cdot 0 = 0 \\ & (0,1) & \longmapsto & 1 \cdot 0 = 0 \\ & (1,0) & \longmapsto & 0 \cdot 1 = 0 \\ & (1,1) & \longmapsto & 1 \cdot 1 = 1 \end{array}$$

Efectivamente, las funciones booleanas $\tilde{p}_B$ y $\tilde{q}_B$ coinciden.

Notas: (1) Cuando se considera el álgebra de Boole $\mathbb{B}$, como en el ejemplo anterior, abreviaremos la notación $\tilde{p}_{\mathbb{B}}$ por $\tilde{p}$.

(2) Dado $\mathscr{P}_n$, las funciones booleanas definidas a partir de $\mathscr{P}_n$ sobre el álgebra de Boole $\mathbb{B}$ pueden ser dotadas de estructura de álgebra de Boole (¡ejercicio!); se representa por $\mathscr{P}_n(\mathbb{B})$.

Una observación clave es que polinomios booleanos diferentes pueden dar lugar a la misma función booleana:

Definición. Dos polinomios booleanos p y q en $\mathscr{P}_n$, se dice que son *equivalentes* si representan la misma función booleana, es decir, si $\tilde{p} = \tilde{q}$. Se escribe $p \sim q$.

Obsérvese también que la equivalencia de polinomios booleanos es una relación de equivalencia (es un buen ejercicio comprobarlo). De hecho, sobre el conjunto cociente $\mathscr{P}_n / \sim$ se pueden definir sendas operaciones que le dotan de estructura de álgebra de Boole isomorfa a $\mathscr{P}_n(\mathbb{B})$.

Ejemplo. La función booleana anterior $f(x,z,y) = x + xy + \bar{y}z$ es la misma que la dada por el polinomio booleano $x + \bar{y}z$ (basta aplicar la ley (B7)(a) de absorción). Dicho de otra manera, las expresiones booleanas $x + xy + \bar{y}z$ y $x + \bar{y}z$ son equivalentes. Escribimos $x + xy + \bar{y}z \sim x + \bar{y}z$.

Desde este punto de vista surgen dos preguntas de manera natural:

Pregunta 1): ¿Cómo saber si dos polinomios booleanos distintos corresponden a la misma función booleana? En concreto, ¿cómo elegir un representante natural?

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Pregunta 2): ¿Cómo obtener la expresión más simple posible de una función booleana (en particular, qué significa más simple)?

En lo que resta de capítulo responderemos a la primera de las cuestiones, reservando la segunda a los capítulos siguientes. Estamos, pues, interesados en cómo son las clases de equivalencia respecto de la relación $\sim$ anterior. En este sentido, definamos:

Definición. Un *sistema de formas normales* de $\mathscr{P}_n$ es un conjunto $N \subseteq \mathscr{P}_n$ tal que

(a) Para cualquier $p \in \mathscr{P}_n$ existe $q \in N$ tal que $p \sim q$;
(b) Si $q_1, q_2 \in N$ son tales que $q_1 \sim q_2$, entonces $q_1 = q_2$.

Es decir, N tiene un único representante de cada clase de $\mathscr{P}_n / \sim$.

Notación: Escribiremos a partir de ahora $x^0 := \bar{x}$ y $x^1 := x$, tanto si x es una indeterminada como si es un elemento de una álgebra de Boole. Con estas definiciones, en el álgebra de Boole $\mathbb{B} = \{0,1\}$, dados $a, b \in \mathbb{B}$ es trivial comprobar que $a^b = 1$ si y solamente si $a = b$.

Veamos un primer ejemplo de sistema de formas normales.

Definición. Definimos el conjunto

$$N_d := \left\{ \sum_{(i_1,\ldots,i_n)\in\mathbb{B}^n} d_{i_1\ldots i_n} x_1^{i_1} \cdots x_n^{i_n} : d_{i_1\ldots i_n} \in \mathbb{B} \right\}.$$

Los sumandos en $\sum d_{i_1\ldots i_n} x_1^{i_1} \cdots x_n^{i_n}$ se consideran ordenados por el orden lexicográfico, es decir:

$$(i_1,\ldots,i_n) < (j_1,\ldots,j_n) \iff \exists k \text{ con } i_1 = j_1,\ldots,i_k = j_k \text{ e } i_{k+1} < j_{k+1}.$$

Por ejemplo, para $n = 2$ y considerando las indeterminadas x, y, los posibles pares $(i, j) \in \mathbb{B}^2$ son obviamente $(0,0), (0,1), (1,0), (1,1)$, y así los monomios que aparecen en N_d son

$$x^0y^0 = \bar{x}\bar{y},\ x^0y^1 = \bar{x}y,\ x^1y^0 = x\bar{y},\ x^1y^1 = xy,$$

luego en este caso particular N_d es de la forma

$$N_d = \left\{ d_{00}\bar{x}\bar{y} + d_{01}\bar{x}y + d_{10}x\bar{y} + d_{11}xy : d_{ij} \in \mathbb{B} \right\}.$$

La siguiente observación es clave para poder demostrar que N_d es un sistema de formas normales:

Observación: Sea el polinomio booleano $p = \sum_{(i_1,\ldots,i_n)\in\mathbb{B}^n} d_{i_1\ldots i_n} x_1^{i_1}\cdots x_n^{i_n}$, entonces la función booleana $\tilde{p}:\mathbb{B}^n \to \mathbb{B}$ está definida por

$$\tilde{p}(a_1,\ldots,a_n) = \underbrace{\sum_{(i_1\ldots i_n)\in\mathbb{B}^n} d_{i_1\ldots i_n} a_1^{i_1}\cdots a_n^{i_n}}_{\in\mathbb{B}} = d_{a_1\ldots a_n} a_1^{a_1}\cdots a_n^{a_n} = d_{a_1\ldots a_n}$$

para cada $(a_1,\ldots,a_n)\in\mathbb{B}^n$. (Hemos aplicado los convenios de exponenciación en $\mathbb{B}$ expuestos anteriormente).

Teorema 8.1. *El conjunto N_d es un sistema de formas normales de $\mathscr{P}_n$.*

Demostración. Hemos de verificar las dos condiciones de la definición de sistema de formas normales:

(a) Sea $p\in\mathscr{P}_n$, tenemos que probar la existencia de un $q\in N_d$ tal que $\tilde{p}=\tilde{q}$. Para ello, basta tomar

$$q = \sum_{(i_1,\ldots,i_n)\in\mathbb{B}^n} d_{i_1\ldots i_n} x_1^{i_1}\cdots x_n^{i_n} \;\text{ con } d_{i_1\ldots i_n} = \tilde{p}(i_1,\ldots,i_n).$$

Así, por la observación anterior,

$$\tilde{q}(i_1,\ldots,i_n) = d_{i_1\ldots i_n} = \tilde{p}(i_1,\ldots,i_n),$$

luego $\tilde{p}=\tilde{q}$ y entonces $p\sim q$.

(b) Si $q_1,q_2\in N_d$ con $q_1\sim q_2$, veamos que $q_1=q_2$. Para ello, si escribimos

$$q_1 = \sum d_{i_1\ldots i_n} x_1^{i_1}\cdots x_n^{i_n}$$
$$q_2 = \sum f_{i_1\ldots i_n} x_1^{i_1}\cdots x_n^{i_n},$$

entonces

$$d_{i_1\ldots i_n} = \tilde{q}_1(i_1,\ldots,i_n) = \tilde{q}_2(i_1,\ldots,i_n) = f_{i_1\ldots i_n}$$

y, de esta forma, $q_1=q_2$, como queríamos.

□

Definición. (1) N_d se denomina *sistema de formas normales disyuntivas* de $\mathscr{P}_n$. (2) Para $p\in\mathscr{P}_n$, el único $q\in N_d$ tal que $q\sim p$ se llama *forma normal disyuntiva* de p.

Una cuestión notacional: escribiremos $x_1^{i_1}\cdots x_n^{i_n}$ en vez de $1\cdot x_1^{i_1}\cdots x_n^{i_n}$, y los términos de la forma $0\cdot x_1^{i_1}\cdots x_n^{i_n}$ los suprimiremos de la forma normal disyuntiva.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Ejemplo. Calculemos la forma normal disyuntiva q del polinomio booleano

$$p = x_1(\overline{x_2 + x_3}) + \bar{x}_1 + \bar{x}_3.$$

Será de la forma

$$\begin{aligned} q =& d_{000}\bar{x}_1\bar{x}_2\bar{x}_3 + d_{001}\bar{x}_1\bar{x}_2x_3 + d_{010}\bar{x}_1x_2\bar{x}_3 + d_{011}\bar{x}_1x_2x_3 \\ &+ d_{100}x_1\bar{x}_2\bar{x}_3 + d_{101}x_1\bar{x}_2x_3 + d_{110}x_1x_2\bar{x}_3 + d_{111}x_1x_2x_3, \end{aligned}$$

donde $d_{ijk} = \tilde{p}(i,j,k)$. Calculemos, pues, $\tilde{p}$:

$\mathbf{x_1}$	$\mathbf{x_2}$	$\mathbf{x_3}$	$\tilde{\mathbf{p}}$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

Luego la forma normal disyuntiva buscada es

$$\begin{aligned} q =& 1\cdot\bar{x}_1\bar{x}_2\bar{x}_3 + 1\cdot\bar{x}_1\bar{x}_2x_3 + 1\cdot\bar{x}_1x_2\bar{x}_3 + 1\cdot\bar{x}_1x_2x_3 \\ &+ 1\cdot x_1\bar{x}_2\bar{x}_3 + 0\cdot x_1\bar{x}_2x_3 + 1\cdot x_1x_2\bar{x}_3 + 0\cdot x_1x_2x_3, \end{aligned}$$

es decir,

$$\begin{aligned} q =& \bar{x}_1\bar{x}_2\bar{x}_3 + \bar{x}_1\bar{x}_2x_3 + \bar{x}_1x_2\bar{x}_3 + \bar{x}_1x_2x_3 \\ & x_1\bar{x}_2\bar{x}_3 + x_1x_2\bar{x}_3. \end{aligned}$$

Presentamos un nombre para los sumandos de la forma normal disyuntiva:

Definición. (1) Un polinomio booleano de la forma

$$d_{i_1\ldots i_n}x_1^{i_1}\cdots x_n^{i_n}$$

se llama *minterm*, *mintérmino* o también *término mínimo* (de orden n).
(2) Se dice que $x_1^{i_1}\cdots x_n^{i_n}$ es un minterm de p si aparece en la forma normal disyuntiva de p, es decir, si $\tilde{p}(i_1,\ldots,i_n) = 1$.

Los minterms se denotan con una “m”:

$$m(i_1,\ldots,i_n) = x_1^{i_1}\cdots x_n^{i_n}.$$

Por ejemplo,

$$\bar{x}\bar{y}z + x\bar{y}z = m(0,0,1) + m(1,0,1).$$

Por otra parte, también se denotan aprovechando la escritura en base 10 del número que en base 2 tiene como representación $i_1 \dots i_n$, $i_j \in \mathbb{B}$; para ello aplicamos la conversión de una base en la otra:

$$i_1 \dots i_n = i_1 \cdot 2^{n-1} + \cdots + i_{n-1} \cdot 2 + i_n =: r.$$

Así, escribiremos $m(r) = m(i_1, \dots, i_n)$. Por ejemplo, para $n = 3$ tenemos

$\mathbf{i_1}$	$\mathbf{i_2}$	$\mathbf{i_3}$	**r**
0	0	0	0
0	0	1	1
0	1	0	2
0	1	1	3
1	0	0	4
1	0	1	5
1	1	0	6
1	1	1	7

Por ejemplo,

$$m(3) + m(6) = m(0,1,1) + m(1,1,0) = \bar{x}yz + xy\bar{z}.$$

A veces también escribimos m_r y $m_{i_1 \dots i_n}$ en vez de $m(r)$ y $m(i_1, \dots, i_n)$.

La forma normal disyuntiva no es la única forma de definir formas normales. El conjunto

$$N_c := \left\{ \prod_{(i_1,\dots,i_n) \in \mathbb{B}^n} c_{i_1 \dots i_n} + \bar{x}_1^{i_1} + \cdots + \bar{x}_n^{i_n} : c_{i_1 \dots i_n} \in \mathbb{B} \right\}$$

también es un sistema de formas normales, denominado *sistema de formas normales conjuntivas* de $\mathscr{P}_n$. Además, para $p \in \mathscr{P}_n$ existe un único $q \in N_c$ tal que $q \sim p$, que se llama *forma normal conjuntiva* de p.

Por ejemplo, para $n = 2$ y considerando las indeterminadas x, y, los posibles pares $(i, j) \in \mathbb{B}^2$ son obviamente $(0,0), (0,1), (1,0), (1,1)$, y así los monomios que aparecen en N_c son

$$\bar{x}^0 + \bar{y}^0 = x + y,\ \bar{x}^0 + \bar{y}^1 = x + \bar{y},\ \bar{x}^1 + \bar{y}^0 = \bar{x} + y,\ \bar{x}^1 + \bar{y}^1 = \bar{x} + \bar{y},$$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

luego, en esta situación, N_c es de la forma

$$N_c = \left\{(c_{00}+x+y)\cdot(c_{01}+x+\bar{y})\cdot(c_{10}+\bar{x}+y)\cdot(c_{11}+\bar{x}+\bar{y}) : c_{ij}\in\mathbb{B}\right\}.$$

En este caso también denotaremos $0+x_1^{i_1}+\cdots+x_n^{i_n} =: x_1^{i_1}+\cdots+x_n^{i_n}$, y los factores de la forma $1+x_1^{i_1}+\cdots+x_n^{i_n}$ se suprimen de la forma normal conjuntiva. Además, un polinomio de la forma $c_{i_1\ldots i_n}+x_1^{i_1}+\cdots+x_n^{i_n}$ se llama *maxterm* o *maxtérmino*, o también *término máximo* (de orden n). Para los maxterms se emplea como notación una "M":

$$M(i_1,\ldots,i_n) := \bar{x}_1^{i_1}+\cdots+\bar{x}_n^{i_n}.$$

Por ejemplo, $M(1,1,0)=\bar{x}+\bar{y}+z$.

Se dice que $x_1^{i_1}+\cdots+x_n^{i_n}$ es un maxterm de p si aparece en la forma normal conjuntiva de p, es decir, si

$$\tilde{p}(i_1,\ldots,i_n)=0.$$

Los detalles relativos a las formas normales conjuntivas se dejan al lector, teniendo en cuenta que su estudio es totalmente análogo al de las formas normales disyuntivas. Veamos otro ejemplo de formas normales:

Ejemplo. Sea $p=xy+\bar{x}$ un polinomio booleano de orden 2. La "tabla de verdad" (abusando del lenguaje) que define la función booleana $\tilde{p}$ es

x	**y**	$\mathbf{\tilde{p}(x,y)}$
1	1	**1**
1	0	0
0	1	**1**
0	0	**1**

Los valores "1" corresponden a los minterms m_{11}, m_{01} y m_{00}, luego la forma normal disyuntiva de p es

$$q=m_{11}+m_{01}+m_{00}=xy+\bar{x}y+\bar{x}\bar{y}.$$

El cálculo de la forma normal conjuntiva se realiza de forma análoga (dual); ahora se han de considerar los valores "0" de la "tabla de verdad" anterior:

x	**y**	$\mathbf{\tilde{p}(x,y)}$
1	1	1
1	0	**0**
0	1	1
0	0	1

El único valor “0” corresponde al maxterm M_{10}, luego la forma normal conjuntiva de p es

$$q = M_{10} = \bar{x} + y.$$

De manera alternativa, las formas normales conjuntivas y disyuntivas se pueden calcular también aplicando las leyes que rigen en las álgebras de Boole. Veámoslo con ayuda de un ejemplo.

Ejemplo. Sea la expresión booleana

$$p = (\overline{\bar{x} \cdot \bar{y} \cdot z})(\overline{(\bar{x} + z)(\bar{y} + \bar{z})}).$$

Se quiere calcular su forma normal disyuntiva. Lo hacemos en cinco pasos:

(1) Transformación de la expresión en sumas y productos de literales, usando las leyes de *de Morgan* y de involución:

$$\begin{aligned} p = & (\overline{\bar{x}\bar{y}z})(\overline{(\bar{x}+z)(\bar{y}+\bar{z})}) \\ & \sim (\overline{(\bar{x}+\bar{y})z})((\overline{\bar{x}+z}) + \overline{\bar{y}+\bar{z}}) \\ & \sim ((\overline{\bar{x}+\bar{y}}) + \bar{z})((\bar{\bar{x}}\bar{z}) + \bar{\bar{y}}\,\bar{\bar{z}})) \\ & \sim ((\bar{\bar{x}}\,\bar{\bar{y}}) + \bar{z})((\bar{\bar{x}}\bar{z}) + \bar{\bar{y}}\,\bar{\bar{z}})) \\ & \sim (xy + \bar{z})(x\bar{z} + yz). \end{aligned}$$

(2) Transformación en suma de productos aplicando las leyes distributivas:

$$\begin{aligned} p \sim & (xy + \bar{z})(x\bar{z}) + (xy + \bar{z})(yz) \\ & \sim xyx\bar{z} + \bar{z}x\bar{z} + xyyz + \bar{z}yz. \end{aligned}$$

(3) Transformación en suma de productos sin repetición de literales o ceros aplicando las leyes conmutativas, de idempotencia y de complemento:

$$p \sim xy\bar{z} + x\bar{z} + xyz + 0. \qquad (*)$$

(4) Transformación en forma disyuntiva aplicando las leyes de absorción e identidad: Observamos en la expresión $(*)$ que el producto $x\bar{z}$ está contenido en $xy\bar{z}$, por lo que una de las leyes de absorción, junto a la conmutatividad, permite escribir

$$x\bar{z} + xy\bar{z} \sim x\bar{z} + x\bar{z}y \sim x\bar{z}$$

y se puede “borrar” $xy\bar{z}$ de la suma en $(*)$. Además, una de las leyes de identidad posibilita el “borrado” de 0 en $(*)$. Así queda

$$p \sim x\bar{z} + xyz.$$

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

En los monomios de $x\bar{z}+xyz$ todavía no aparecen todas las variables posibles: en $x\bar{z}$ falta o bien y o bien $\bar{y}$, por lo que necesitamos un último paso que repare esta situación.

(5) Aplicación de las leyes de complemento (B4)(a), es decir $x+\bar{x}=1$, y de idempotencia (B5)(a), es decir $x+x=x$, de forma que

$$\begin{aligned} p &\sim x\bar{z}1+xyz \\ &\sim x\bar{z}(y+\bar{y})+xyz \\ &\sim x\bar{z}y+x\bar{z}\bar{y}+xyz \\ &\sim xy\bar{z}+x\bar{y}\bar{z}+xyz. \end{aligned}$$

La forma normal disyuntiva de p es $x\bar{z}y+x\bar{z}\bar{y}+xyz$.

En los capítulos siguientes nos ocuparemos de la "Pregunta 2)", relativa a la simplificación de polinomios booleanos.

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

[Conr] Conradie, W., Goranko, V.: Logic and Discrete Mathematics. A concise introduction. Wiley, 2015
[FG] Ferrando, J.C., Gregori, V.: Matemática Discreta. 2. ed. Reverté, 2002
[Gall] Gallier, J.: Discrete Mathematics. Springer, 2011
[Ham] Hamilton, A.G.: Logic for mathematicians, Cambridge U.P. 1978
[LiPi] Lidl, R., Pilz, G.: Applied Abstract Algebra. Second edition. Springer, 1998
[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3. ed. McGraw Hill, 2007
[Rios] Ríos, S.: Matemática finita. Paraninfo, 1974
[Smull] Smullyan, R.M.: A Beginner's guide to Mathematical Logic. Dover, 2014
[Wall2] Wallis, W.D.: A beginner's guide to discrete mathematics. Second edition. Birkhäuser, 2012

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Capítulo 9. Simplificación de polinomios booleanos

En este capítulo y el siguiente responderemos a la pregunta 2) efectuada en el capítulo anterior:

¿Cómo obtener la expresión más simple posible de un polinomio booleano?

En primer lugar definamos una noción de simplicidad de polinomios. Para ello necesitamos algunas definiciones previas.

Definición. (1) Un *literal* es un polinomio booleano en $\mathscr{P}_n$ que consta de una sola variable, es decir, 0, 1, $x_1,\ldots,x_n,\bar{x}_1,\ldots,\bar{x}_n$. Una *expresión producto* o *producto fundamental* es un literal o un producto de dos o más literales donde ningún par de literales contiene la misma variable.
(2) Llamaremos *expresión suma de produtos* a un polinomio del tipo

$$\sum_{i\in I} p_i$$

donde cada p_i es un producto fundamental. Los sumandos p_i se llaman *términos* de la expresión suma de productos.
(3) Un *subproducto* de un producto fundamental p es un producto fundamental q tal que los literales de p también lo son de q. A veces se utiliza la expresión "p está contenido en q".

Ejemplo. Son ejemplos de literales x, ó $\bar{y}$. Las expresiones xy, $\bar{x}yz$ son productos fundamentales; los polinomios booleanos $x+y\bar{z}$, $yz\bar{z}$, $x\bar{x}$, en cambio, no lo son. Por otra parte, xy es subproducto de xzy, pero no de $\bar{y}z$.

Obsérvese que cualquier producto se puede expresar como un producto fundamental: si contiene dos veces un mismo literal, digamos x, podemos reemplazar xx por x merced a la ley de idempotencia (B5)(b); si contiene x y $\bar{x}$, la ley de complemento (B4)(b) permite reemplazar su producto y, de hecho, todo el producto donde pueda estar contenido, por 0, como en

$$xzy\bar{x} \overset{(B1)}{\sim} x\bar{x}zy \overset{(B4)}{\sim} 0zy \overset{(B6)}{\sim} 0.$$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Nota: Sea p un polinomio booleano. Una *forma disyuntiva* de p es una expresión dada por un producto fundamental o una suma de dos o más productos fundamentales tales que ninguno de ellos está contenido en otro, y tal que sea equivalente a p. Cuando en la forma disyuntiva aparecen todas las variables posibles, entonces se trata de la forma normal disyuntiva.

Ejemplo. La expresión $p = x\bar{z} + \bar{y}z + xy\bar{z}$ es una suma de productos fundamentales, pero *no* una forma disyuntiva, pues $x\bar{z}$ está contenido en $xy\bar{z}$. Sin embargo, admite una forma disyuntiva equivalente aplicando la ley de absorción (B7)(a), es decir, la de la forma $a + (a \cdot b) = a$:

$$p \sim x\bar{z} + \bar{y}z + xy\bar{z} \overset{(B1)}{\sim} x\bar{z} + \bar{y}z + y\bar{z}x \overset{(B7)}{\sim} x\bar{z} + \bar{y}z.$$

Definición. Dadas dos expresiones suma de productos p y q, se dice que *p es más simple que q* si

(i) p tiene menos sumandos que q;
(ii) p tiene el mismo número de sumandos que q pero menos literales (contados con repeticiones).

En el conteo, se prescinde de los literales 0 y 1.

Por ejemplo, dadas $p = xy + x\bar{y}z + \bar{x}yz$ y $q = xt$, la expresión p tiene 3 sumandos y 8 literales, en tanto que q tiene un solo sumando y 2 literales, luego q es más simple que p.

Definición. Se dice que una expresión suma de productos p es *minimal* si no existe otra expresión suma de productos q equivalente a p y más simple que p.

Minimalidad no implica unicidad, como veremos después.

¿Cómo encontrar expresiones suma de productos minimales? Empecemos dando una definición aparentemente aislada del contexto:

Definición. Sean $p, q \in \mathscr{P}_n$ dos polinomios booleanos.
(1) Se dice que p es *implicante* de q siempre que, si $\tilde{p}(i_1, \ldots, i_n) = 1$, entonces también $\tilde{q}(i_1, \ldots, i_n) = 1$, es decir,

$$\tilde{p}(i_1, \ldots, i_n) \implies \tilde{q}(i_1, \ldots, i_n).$$

(2) Se dice que p es un *implicante primo* de q si

(i) p es un producto fundamental,
(ii) p es implicante de q,
(iii) ningún subproducto de p es implicante de q.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

En otras palabras, si $p+q \sim q$ y además ningún otro producto fundamental contenido en p cumple esta propiedad.

¿Cómo probar, pues, que un cierto producto fundamental p es un implicante primo de una expresión q? De acuerdo con la definición anterior se han de realizar dos comprobaciones:

(i) manipular $p+q$ aplicando operaciones booleanas para mostrar que es equivalente a q;
(ii) ver que todo producto fundamental p' incluido en p verifica que $p'+q$ no es equivalente a q; esto se suele hacer mostrando que hay alguna asignación de valores a las variables de la que resultan diferentes valores para $p'+q$ y q.

Ejemplo. Veamos que xz es un implicante primo de $q = xy + x\bar{y}z + \bar{x}yz$. Para ello ejecutamos los dos pasos que acabamos de describir:

(i) Se tiene que $xz+q \sim q$ ya que:

$$\begin{aligned} xz+q \sim & xz+xy+x\bar{y}z+\bar{x}yz \\ & \sim x(y+\bar{y})z+xy+x\bar{y}z+\bar{x}yz \\ & \sim xyz+x\bar{y}z+xy+x\bar{y}z+\bar{x}yz \\ & \sim (xy+xyz)+(x\bar{y}z+x\bar{y}z)+\bar{x}yz \\ & \sim xy+x\bar{y}z+\bar{x}yz \\ & \sim q. \end{aligned}$$

(ii) Los únicos productos fundamentales incluidos en xz son x y z. Hay que comprobar que $x+q$ no es equivalente a q y que $z+q$ tampoco es equivalente a q. Para ver en primer lugar que $x+q$ no es equivalente a q basta observar que si $x = 1$ e $y = z = 0$, entonces $x+q = 1 \neq 0 = q$; y para ver que $z+q$ no es equivalente a q, se toma $z = 1$ y $x = y = 0$, y así es $z+q = 1 \neq 0 = q$.

Los implicantes primos son muy importantes en nuestro marco:

Teorema 9.1. *Si q es una expresión suma de productos minimal, entonces los términos de q son implicantes primos de q.*

Así, una expresión suma de productos minimal es la suma de sus implicantes primos, por lo que construir una expresión suma de productos minimal de un polinomio booleano es encontrar sus implicantes primos.

Puede ocurrir que en una expresión suma de productos se puedan eliminar algunos términos "superfluos":

Definición. Una expresión suma de productos $p = \sum_{i\in I} r_i$ se llama *irredundante* si no existe ningún sumando tal que al suprimirlo se obtenga otra expresión suma de productos equivalente a p; es decir, si no existe $i_0 \in I$ tal que p es equivalente a $\sum_{i\in I,\ i\neq i_0} r_i$.

Irredundancia y minimalidad son dos conceptos relacionados en el sentido del siguiente resultado:

Teorema 9.2. (a) *Si una expresión suma de productos p es minimal, entonces es suma irredundante de implicantes primos de p.*

(b) *Todo polinomio booleano es equivalente a la suma de sus implicantes primos.*

Lo que dice el primer aserto es que para todo $i_0 \in I$, p no es equivalente a $\sum_{i\in I,\ i_0\neq i} q_i$ (es decir, p es irredundante), y que para todo $i \in I$, q_i es implicante primo de p. Si se quisieran demostrar los resultados anteriores, sería útil conocer las propiedades siguientes (cuya justificación también omitimos):

(a) Todo sumando de $p \in \mathscr{P}_n$ es implicante de p.
(b) q es implicante de p si y solamente si todos los minterms de q son minterms de p.
(c) Si p es un producto fundamental y q es un subproducto de p, entonces p es implicante de q.
(d) Si q es un producto fundamental implicante de p, entonces todo múltiplo de q también es implicante de p.

Por tanto, en lo que resta de capítulo y en el siguiente, dada una expresión suma de productos p se desea:

(a) Encontrar todos los implicantes primos de p; para esto se explicarán el *método de los consensos* (a continuación), el *método de Veitch-Karnaugh* y el *algoritmo de Quine*.
(b) A partir de todos los implicantes primos, encontrar sumas irredundantes; este problema se soluciona con un algoritmo conocido como *cuadrícula de McCluskey*.
(c) De entre las sumas irredundantes, buscar alguna que sea minimal.

El método de los consensos. Comencemos por describir el llamado método de los consensos para calcular los implicantes primos de una expresión suma de productos p. Se basa en la observación siguiente: para $p,q,r \in \mathscr{P}_n$

$$pq+\bar{p}r \sim pq+\bar{p}r+qr.$$

El término qr se denomina *consenso* (relativo a p) de pq y $\bar{p}r$.

Algoritmo de los consensos

Entrada: Un polinomio booleano $p \in \mathscr{P}_n$ escrito en expresión suma de productos (no necesariamente en forma normal disyuntiva).
Inicialización: $p_0 := p$.
Etapa i-ésima: Para $1 \geq i \geq n$, se añaden a p_{i-1} todos los consensos relativos a x_i obtenidos a partir de pares de sumandos de p_{i-1}. Se simplifican estos consensos teniendo en cuenta que $x_j\bar{x}_j \sim 0$ y que $x_jx_j \sim x_j$. Aplicando la ley de absorción, se eliminan de la expresión resultante todos aquellos productos para los que existe un subproducto en dicha expresión. El polinomio booleano resultante se denota por p_i.
Salida: p_n.

Veamos un sencillo ejemplo de aplicación de este algoritmo.

Ejemplo. Sea $p = vx+xy+v\bar{y}+\bar{v}yz+\bar{v}\bar{x}\bar{z}+\bar{v}\bar{x}y \in \mathscr{P}_4$.

Etapa 1:

(a) Consensos no nulos en $p_0 = p$ relativos a v: xyz y $\bar{x}\bar{y}\bar{z}$.
(b) Términos absorbidos: xyz por xy.
(c) $p_1 = p+xyz+\bar{x}\bar{y}\bar{z} \sim vx+xy+v\bar{y}+\bar{v}yz+\bar{v}\bar{x}\bar{z}+\bar{v}\bar{x}y+\bar{x}\bar{y}\bar{z}$.

Etapa 2:

(a) Consensos en p_1 relativos a x: $v\bar{y}\bar{z}$, $\bar{v}y\bar{z}$, $\bar{v}y$.
(b) Términos absorbidos: $\bar{v}yz$, $\bar{v}\bar{x}y$,$\bar{v}y\bar{z}$ por $\bar{v}y$; $v\bar{y}\bar{z}$ por $v\bar{y}$.
(c) $p_2 = p_1+v\bar{y}\bar{z}+\bar{v}y\bar{z}+\bar{v}y \sim vx+xy+v\bar{y}+\bar{v}y+\bar{v}\bar{x}\bar{z}+\bar{x}\bar{y}\bar{z}$.

Etapa 3:

(a) Consensos en p_2 relativos a y: vx y $\bar{v}\bar{x}\bar{z}$, que ya están en p_2.
(b) Términos absorbidos: ninguno.

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

(c) $p_3 = p_2 + vx + \bar{v}\bar{x}\bar{z} \sim p_2$.

Etapa 4:

(a) Consensos en p_3 relativos a z: ninguno.
(b) Términos absorbidos: ninguno.
(c) $p_4 = p_3 = p_2$.

Salida: $p_4 = vx + xy + v\bar{y} + \bar{v}y + \bar{v}\bar{x}\bar{z} + \bar{x}\bar{y}\bar{z}$.

Se podría demostrar:

Teorema 9.3. *La salida del algoritmo de los consensos es la suma de todos los implicantes primos de p.*

Ahora bien, la suma de todos los implicantes primos de p no es, en general, la forma minimal.

En el capítulo siguiente analizaremos otros dos métodos de simplificación, a saber, el método de Quine-McCluskey y el de Veitch-Karnaugh.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

[Conr] Conradie, W., Goranko, V.: Logic and Discrete Mathematics. A concise introduction. Wiley, 2015
[FG] Ferrando, J.C., Gregori, V.: Matemática Discreta. 2. ed. Reverté, 2002
[GOV] Galindo Pastor, C., Orús Báguena, M.P., Vindel Cañas, M.P.: Problemes de matemàtica discreta. Universitat Jaume I, 1997
[Gall] Gallier, J.: Discrete Mathematics. Springer, 2011
[Ham] Hamilton, A.G.: Logic for mathematicians, Cambridge U.P. 1978
[LiPi] Lidl, R., Pilz, G.: Applied Abstract Algebra. Second edition. Springer, 1998
[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3. ed. McGraw Hill, 2007
[Rios] Ríos, S.: Matemática finita. Paraninfo, 1974
[Smull] Smullyan, R.M.: A Beginner's guide to Mathematical Logic. Dover, 2014
[Wall2] Wallis, W.D.: A beginner's guide to discrete mathematics. Second edition. Birkhäuser, 2012

Capítulo 10. Métodos de simplificación

En este capítulo presentamos los métodos de simplificación de polinomios booleanos llamados de Veitch-Karnaugh y de Quine–McCluskey, que en realidad son tres algoritmos: el de Veitch-Karnaugh, el algoritmo de Quine para el cálculo de implicantes primos (que es una alternativa al método de Veitch-Karnaugh para orden arbitrario, es decir, para un número cualquiera de variables), y la cuadrícula de McCluskey, que toma la salida del método de Veitch-Karnaugh o del algoritmo de Quine y los convierte en sumas irredundantes (es decir, desecha los implicantes primos superfluos, si los hubiera).

Ahora bien, ¿cómo encontrar implicantes primos de forma efectiva? Existe un método visual muy útil para simplificar expresiones booleanas con un número no muy elevado de variables (nosotros lo veremos para dos, tres y cuatro), llamado *método de los diagramas de Veitch-Karnaugh* o *método de Veitch-Karnaugh*. Fue propuesto en 1952 por Edward W. VEITCH (1924–2013) y desarrollado al año siguiente por Maurice KARNAUGH (1924) en su etapa en los laboratorios Bell.

Definición. Dos productos fundamentales p_1 y p_2 se llaman *adyacentes* si tienen las mismas variables y difieren exactamente en un literal.

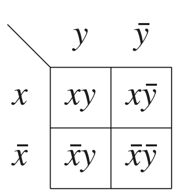
Es decir, aparece una variable no complementada en uno de los productos fundamentales y complementada en el otro.

Ejemplo. Los productos fundamentales $p_1 = xy\bar{z}$ y $p_2 = x\bar{y}\bar{z}$ son adyacentes. Los productos $q_1 = \bar{x}yzt$ y $q_2 = xy\bar{z}t$ no son adyacentes, pues difieren en dos literales. Por último, los productos $r_1 = xy\bar{z}$ y $r_2 = xy\bar{z}t$ tampoco son adyacentes, ya que tienen variables diferentes.

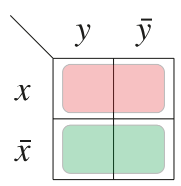
Diagrama de Veitch-Karnaugh de dos variables:

Se trata de una cuadrícula 2×2, es decir, con cuatro entradas, cada una de las cuales representa uno de los cuatro posibles minterms $xy, x\bar{y}, \bar{x}y, \bar{x}\bar{y}$:

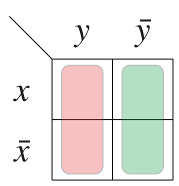
ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170



En el diagrama, los literales x y $\bar{x}$ están representados por los cuadrados coloreados de la figura:



y los literales y e $\bar{y}$ por



Cualquier forma normal disyuntiva q es suma de minterms, por tanto, se representa en el diagrama mediante la selección de los cuadrados de la cuadrícula apropiados.

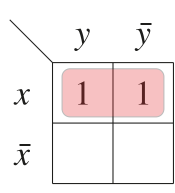
Un implicante primo se representa por un par de cuadrados (minterms) adyacentes a q o un cuadrado aislado, es decir, un cuadrado que no es adyacente a ningún otro (nótese que el concepto de adyacencia de minterms adquiere un significado visual como adyacencia de cuadrados en la cuadrícula).

Una forma disyuntiva minimal para q consistirá en un número mínimo de implicantes primos que recubran a todos los minterms de q, como se ilustra en los ejemplos siguientes. El punto de partida es siempre la forma normal disyuntiva de q, cuyos minterms se señalan en el diagrama por medio de un “1”, por convenio.

Ejemplos. Queremos encontrar los implicantes primos y una forma disyuntiva minimal para cada una de las siguientes expresiones booleanas:

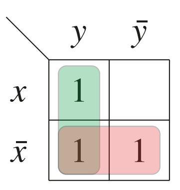
(a) El único implicante primo de $q = xy + x\bar{y}$ es x, dado por el par de cuadrados adyacentes

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170



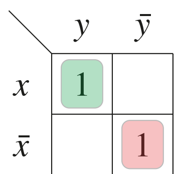
y así x es la forma disyuntiva minimal para q.

(b) Los implicantes primos de $q = xy + \bar{x}y + \bar{x}\bar{y}$ son $\bar{x}$ e y, correspondientes a los dos pares de cuadrados adyacentes



Así, $\bar{x} + y$ es la forma disyuntiva minimal de q.

(c) La expresión booleana $q = xy + \bar{x}\bar{y}$ posee dos implicantes primos minimales, que son exactamente xy y $\bar{x}\bar{y}$; están dados por los dos cuadrados aislados de la figura:



Por tanto, q ya es la forma disyuntiva minimal.

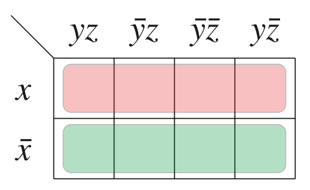
Diagrama de Veitch-Karnaugh de tres variables:

Recordamos que existen en este caso $2^3 = 8$ posibles minterms para tres variables. Se representa en una cuadrícula 2×4:

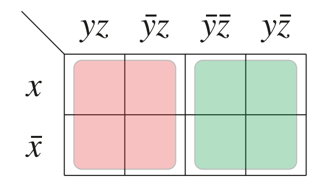
	yz	$\bar{y}z$	$\bar{y}\bar{z}$	$y\bar{z}$
x	xyz	$x\bar{y}z$	$x\bar{y}\bar{z}$	xyz
$\bar{x}$		$\cdots$	$\cdots$	

La figura anterior muestra la correspondencia entre las casillas y los diferentes posibles minterms. En este caso, la visualización de minterms adyacentes viene dada por adyacencia de casillas en el sentido siguiente:

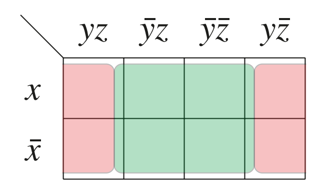
(i) El literal x resp. $\bar{x}$ está representado por la fila superior resp. inferior:



(ii) El literal y resp. $\bar{y}$ está representado por cuadrados 2×2 de la izquierda resp. de la derecha:



(iii) El literal z resp. $\bar{z}$ está representado por la siguiente adyacencia (no geométrica en sentido estricto):



Un rectángulo básico (o bloque) en el diagrama es

(a) o bien un cuadrado,
(b) o bien dos cuadrados adyacentes (en el sentido generalizado que acabamos de ver),
(c) o bien cuatro cuadrados que forman un rectángulo 1×4 ó un cuadrado 2×2.

Los rectángulos básicos de tipo (a) corresponden a productos fundamentales de 3 literales; los rectángulos básicos de tipo (b) corresponden a productos fundamentales de 2 literales; los rectángulos básicos de tipo (c) corresponden a productos fundamentales de 1 literal.

Además, el producto fundamental representado por un rectángulo básico es el producto de justo aquellos literales que aparecen en cada casilla del rectángulo básico (es decir, está formado por el producto de aquellos literales que aparecen en todas esas casillas).

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Supongamos que una forma normal disyuntiva q de suma de productos está representada en el diagrama al colocar "1" en los lugares apropiados.

Un implicante primo de q es un rectángulo básico maximal de q, es decir, un rectángulo básico contenido en q que no está contenido en ningún rectángulo básico más grande en q.

Una forma disyuntiva minimal para q consiste en una cubierta maximal de q, es decir, un número minimal de rectángulos básicos maximales de q que juntos incluyen a todos los cuadrados de q.

Ejemplos. Encontrar los implicantes primos y la forma de suma de productos minimal para cada una de las siguientes formas normales disyuntivas:

(a) La forma normal disyuntiva $q = xyz + x\bar{y}z + \bar{x}y\bar{z} + \bar{x}\bar{y}z$ se simplifica a $xz + \bar{y}z + \bar{x}y\bar{z}$ con ayuda del diagrama siguiente:

	yz	$\bar{y}z$	$\bar{y}\bar{z}$	$y\bar{z}$
x	1	1		
$\bar{x}$		1		1

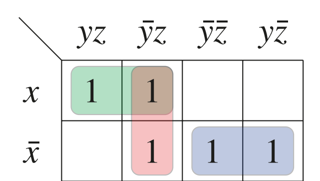
(b) La forma normal disyuntiva $q = xyz + xy\bar{z} + x\bar{y}z + \bar{x}yz + \bar{x}y\bar{z}$ se simplifica a $xz + y$ gracias al diagrama:

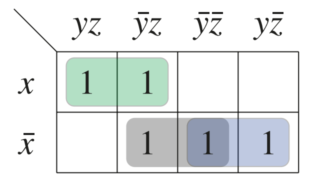
	yz	$\bar{y}z$	$\bar{y}\bar{z}$	$y\bar{z}$
x	1	1		1
$\bar{x}$	1			1

(c) La forma normal disyuntiva $q = xyz + x\bar{y}z + \bar{x}y\bar{z} + \bar{x}\bar{y}\bar{z} + \bar{x}\bar{y}z$ se expresa de manera minimal de dos formas distintas, a saber

$$E = xz + \bar{x}\bar{z} + \bar{y}z = xz + \bar{x}\bar{z} + \bar{x}\bar{y},$$

lo que constituye un ejemplo de la no unicidad de la expresión minimal, de acuerdo a los siguientes diagramas de Veitch-Karnaugh:





ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Diagrama de Veitch-Karnaugh de cuatro variables:

La filosofía es la misma, disponiendo ahora las $2^4 = 16$ posibles minterms en una cuadrícula 4×4:

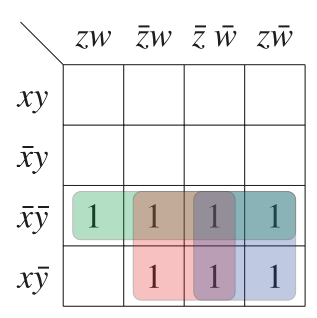
	zw	$\bar{z}w$	$\bar{z}\,\bar{w}$	$z\bar{w}$
xy				
$\bar{x}y$				
$\bar{x}\bar{y}$				
$x\bar{y}$				

Un rectángulo básico es ahora o bien un cuadrado (o casilla) aislado, o bien dos cuadrados adyacentes, o bien cuatro cuadrados que forman un rectángulo de 1×4 ó de 2×2, o bien ocho cuadrados que forman un rectángulo de 2×4. Tales rectángulos corresponden a productos fundamentales con 4, 3, 2 y un literal, respectivamente. De nuevo, los rectángulos básicos maximales corresponderán a los implicantes primos. Téngase en cuenta que ahora por adyacentes se entienden la primera y la cuarta fila, y también la primera y la cuarta columna.

Ejemplo. Los implicantes primos minimales de la expresión booleana

$$q = \bar{x}\bar{y}\bar{z}\bar{w} + \bar{x}\bar{y}\bar{z}w + \bar{x}\bar{y}z\bar{w} + \bar{x}\bar{y}zw + x\bar{y}\bar{z}\bar{w} + x\bar{y}\bar{z}w + x\bar{y}z\bar{w}$$

son $\bar{x}\bar{y}$, $\bar{y}\bar{w}$ e $\bar{y}\bar{z}$, de acuerdo con el diagrama siguiente:



Nota: Se puede aprovechar el diagrama para encontrar sumas irredundantes. Se trata de encontrar una familia de bloques maximales que cubra todos los 1's y que

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

sea minimal en el sentido siguiente: no se puede quitar ningún bloque sin destapar algún 1 (irredundante). Recuérdese también: a igual número de bloques, cuanto más grande sean estos, más simple es el polinomio que se obtiene.

Una alternativa más operativa al método de Veitch-Karnaugh es el algoritmo debido al lógico estadounidense Willard Van Orman QUINE (1908–2000).

Algoritmo 10.1 (Algoritmo de Quine)**.**
Entrada: *Forma normal disyuntiva p.*
Salida: *Implicantes primos de p.*
Descripción:

(1) *Cada sumando lo representamos por* ceros *y* unos*, según la variable aparezca complementada o sin complementar, clasificados en una columna según el número de unos (es decir, de variables sin complementar) que aparezcan.*

(2) *Se suma cada minterm con r* unos *a cada minterm con $r-1$* unos*. Si la suma cancela exactamente un literal, este se substituye con un guion "$-$". Si se cancela más de un literal, esta suma no se tiene en cuenta.*

El resultado de la suma se consigna en otra columna y se marcan con un asterisco "$*$" los dos minterms utilizados como sumandos en la 1ª *columna.*

Si la suma de dos minterms arroja un resultado ya existente, este no se vuelve a consignar, pero se marcarán los cuatro sumandos involucrados con "$*$".

Este proceso se repite mientras sea posible. (En el ejemplo se verá qué significa sumar guiones).

Ilustremos a la vez que detallamos el algoritmo con un ejemplo, en aras de la inteligibilidad. Consideremos para ello un polinomio booleano de orden 4 cuya forma normal disyuntiva es

$$q = \bar{x}\bar{y}\bar{z}\bar{w} + \bar{x}\bar{y}z\bar{w} + \bar{x}\bar{y}zw + \bar{x}yz\bar{w} + \bar{x}yzw + x\bar{y}\bar{z}\bar{w} + x\bar{y}\bar{z}w + xy\bar{z}\bar{w} + xy\bar{z}w + xyz\bar{w} + xyzw.$$

(1) Usando la notación de minterms con subíndice binario se tiene

$$q = m_{0000} + m_{0010} + m_{0011} + m_{0110} + m_{0111} + m_{1000} + m_{1001} + m_{1100} + m_{1101} + m_{1110} + m_{1111}.$$

0	0	0	0
0	0	1	0
1	0	0	0
0	0	1	1
0	1	1	0
1	0	0	1
1	1	0	0
0	1	1	1
1	1	0	1
1	1	1	0
1	1	1	1

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

(2) Escríbase en columna los subíndices de los minterms de q dispuestos como en (1) separados en bloques según el número de unos de su subíndice binario; así, en el ejemplo, el primer bloque consta de 0000, el segundo bloque de 0010 y 1000, etc. como en la tabla anterior.

(3) Considérense todas las parejas de números binarios pertenecientes a bloques contiguos que difieran solamente en un dígito y márquense a la derecha con un asterisco.

(3.1) Yuxtapóngase a esta columna una segunda columna en la que se consignen las expresiones obtenidas al reemplazar el dígito en que difieren por un guion "–", de nuevo por bloques (pues la comparación se ha ido estableciendo por bloques contiguos de la primera columna) de forma que el 1$^{\text{er}}$ bloque de la 2$^{\text{a}}$ columna ataña a resultados de comparaciones entre los bloques 1° y 2° de la 1$^{\text{a}}$ columna, el 2° bloque de la 2$^{\text{a}}$ columna consigne sólo resultados de comparaciones entre expresiones de los bloques 2° y 3° de la 1$^{\text{a}}$ columna, y así sucesivamente.

(3.2) Repítase el proceso entre bloques de la 2$^{\text{a}}$ columna, marcando con un asterisco a la derecha y construyendo una tercera columna como antes; el signo "–" se considerará ahora como un símbolo más para comparar, como si de un 0 o de un 1 se tratara.

(3.3) Repítase el proceso hasta que no se puedan añadir nuevas columnas (porque todos los elementos difieran en más de un símbolo).

En el ejemplo, aplicado todo el paso (3) resulta la siguiente tabla:

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

0 0 0 0 *	0 0 – 0	0 – 1 –
0 0 1 0 *	– 0 0 0	1 – 0 –
1 0 0 0 *	0 0 1 – *	– 1 1 –
0 0 1 1 *	0 – 1 0 *	1 1 – –
0 1 1 0 *	1 0 0 – *	
1 0 0 1 *	1 – 0 0 *	
1 1 0 0 *	0 – 1 1 *	
0 1 1 1 *	0 1 1 – *	
1 1 0 1 *	– 1 1 0 *	
1 1 1 0 *	1 – 0 1 *	
1 1 1 1 *	1 1 0 – *	
	1 1 – 0 *	
	– 1 1 1 *	
	1 1 – 1 *	
	1 1 1 – *	

(4) Escríbanse como suma los minterms correspondientes a los dígitos en binario no marcados con un asterisco: esta suma es la salida del algoritmo.

Continuando con el ejemplo, se deduce que el polinomio booleano q se expresa como suma de los siguientes implicantes primos

$$q \sim m_{00-0} + m_{-000} + m_{0-1-} + m_{1-0-} + m_{-11-} + m_{11--}$$
$$\sim \bar{x}\bar{y}\bar{w} + \bar{y}\bar{z}\bar{w} + \bar{x}z + x\bar{z} + yz + xy.$$

(Estos corresponden a los términos no marcados con "$*$" en la tabla anterior).

Efectivamente, el algoritmo de Quine permite encontrar una expresión muy simple de q, pero podría ser todavía redundante. Para buscar sumas irredundantes se ha de utilizar otro procedimiento conocido como "cuadrícula de McCluskey". Este nombre honra la memoria del ingeniero estadounidense Edwar J. McCluskey (1929–2016).

Algoritmo 10.2 (Cuadrícula de McCluskey)**.**
Entrada: *Forma disyuntiva minimal p.*
Salida: *Expresión suma de productos minimal irredundante equivalente a p.*
Descripción:

(1) *Dispóngase una tabla de doble entrada, donde en cada columna se anotan los minterms (en forma canónica disyuntiva) y en cada fila un implicante primo (de los obtenidos en Veitch-Karnaugh o en Quine).*

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

(2) *Márquense con un aspa las casillas en las que el implicante primo está contenido en el minterm correspondiente.*

(3) *De entre las aspas anteriores, rodéense con un círculo aquéllas que aparezcan solas en toda una columna.*

Esto significa que los minterms correspondientes están contenidos en un único implicante primo; estos implicantes primos conforman el llamado corazón *de p, y aparecen necesariamente en toda expresión minimal irredundante de p (pues de lo contrario habría minterms no contenidos en ningún implicante primo).*

(3) *Márquense los minterms que contienen los implicantes primos del corazón de p.*

(4) *De entre implicantes primos que no estén en el corazón de p, tómense tantos como sean estrictamente necesarios para cubrir los minterms no marcados en (3), es decir, el mínimo número necesario.*

(5) *La suma del corazón de p más los implicantes primos obtenidos en (4) es la expresión minimal irredundante buscada.*

Veamos un ejemplo; en él también se pone de manifiesto que la salida del algoritmo no es única, es decir, puede haber varias posibilidades para que la suma sea irredundante.

Ejemplo. Consideremos la salida del ejemplo anterior, es decir, la forma disyuntiva

$$\begin{aligned} p &= m_{00-0} + m_{-000} + m_{0-1-} + m_{1-0-} + m_{-11-} + m_{11--} \\ &= \bar{x}\bar{y}\bar{w} + \bar{y}\bar{z}\bar{w} + \bar{x}z + x\bar{z} + yz + xy, \end{aligned}$$

y apliquemos los pasos del método de McCluskey que acabamos de describir:

(1) Construyamos una tabla en la que las columnas correspondan a los minterms de la forma normal disyuntiva q de p y las filas a los implicantes primos encontrados:

	0000	0010	0011	0110	0111	1000	1001	1100	1101	1110	1111
00–0											
–000											
0–1–											
1–0–											
–11–											
11– –											

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

(2) Reconocemos qué implicantes primos están contenidos en cada uno de los minterms y señalamos la casilla correspondiente con un aspa "$\times$":

	0000	0010	0011	0110	0111	1000	1001	1100	1101	1110	1111
00–0	$\times$	$\times$									
–000	$\times$					$\times$					
0–1–		$\times$	$\times$	$\times$	$\times$						
1–0–						$\times$	$\times$	$\times$	$\times$		
–11–				$\times$	$\times$					$\times$	$\times$
11– –								$\times$	$\times$	$\times$	$\times$

(3) Determinamos el corazón de p en color rojo:

	0000	0010	0011	0110	0111	1000	1001	1100	1101	1110	1111
00–0	$\times$	$\times$									
–000	$\times$					$\times$					
0–1–		$\times$	$\otimes$	$\times$	$\times$						
1–0–						$\times$	$\otimes$	$\times$	$\times$		
–11–				$\times$	$\times$					$\times$	$\times$
11– –								$\times$	$\times$	$\times$	$\times$

(4) Marcamos en azul los minterms que quedan cubiertos por los implicantes primos del corazón de p:

	0000	0010	0011	0110	0111	1000	1001	1100	1101	1110	1111
00–0	$\times$	$\times$									
–000	$\times$					$\times$					
0–1–		$\times$	$\otimes$	$\times$	$\times$						
1–0–						$\times$	$\otimes$	$\times$	$\times$		
–11–				$\times$	$\times$					$\times$	$\times$
11– –								$\times$	$\times$	$\times$	$\times$

Efectivamente, "$0-1-$" está incluido tanto en 0010, 0011, 0110 y 0111, pues todos ellos fueron marcados con un $\times$ en la fila de "$0-1-$"; de idéntica manera, el implicante primo "$1-0-$" está contenido en los minterms 1000, 1001, 1100 y 1101, pues en su fila aparecen aspas en estas columnas. Todos estos minterms, contenidos en los elementos del corazón, son los coloreados en azul.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Esto quiere decir que tenemos aún por cubrir los minterms que no están marcados en azul por los implicantes primos que no forman parte del corazón, y además de manera minimal. Para ello se aplica el paso (5).

(5) Quedan por cubrir los minterms 0000, 1110 y 1111. Para el 0000 podemos tomar o bien el implicante primo "$00-0$" o bien "-000"; y para cubrir tanto 1110 como 1111 basta tomar o bien "$-11-$" o bien "$11--$", de forma que se obtienen cuatro expresiones minimales (irredundantes) equivalentes a p (y a q) para p, todas ellas igualmente válidas, a saber:

$$\begin{aligned}
p_1 &= m_{0-1-} + m_{1-0-} + m_{00-0} + m_{-11-} = \bar{x}z + x\bar{z} + \bar{x}\bar{y}\bar{w} + yz \\
p_2 &= m_{0-1-} + m_{1-0-} + m_{00-0} + m_{11--} = \bar{x}z + x\bar{z} + \bar{x}\bar{y}\bar{w} + xy \\
p_3 &= m_{0-1-} + m_{1-0-} + m_{-000} + m_{-11-} = \bar{x}z + x\bar{z} + \bar{y}\bar{z}\bar{w} + yz \\
p_4 &= m_{0-1-} + m_{1-0-} + m_{-000} + m_{11--} = \bar{x}z + x\bar{z} + \bar{y}\bar{z}\bar{w} + xy.
\end{aligned}$$

Observación: Hemos visto que se puede aprovechar el diagrama de Veitch-Karnaugh para encontrar sumas irredundantes; si se procede de esa forma, no es necesario aplicar el algoritmo de la cuadrícula de McCluskey a la salida de Veitch-Karnaugh. En este sentido, hagamos notar que el corazón está formado por los bloques maximales tales que existe un 1 que solamente pertenece a uno de los bloques.

Este capítulo termina el área temática de álgebras de Boole de este curso. Aprovechando el ejemplo de estructura algebraica que nos brindan precisamente las álgebras de Boole, ahondaremos en los próximos capítulos en esta noción.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

[Conr] Conradie, W., Goranko, V.: Logic and Discrete Mathematics. A concise introduction. Wiley, 2015

[FG] Ferrando, J.C., Gregori, V.: Matemática Discreta. 2. ed. Reverté, 2002

[GOV] Galindo Pastor, C., Orús Báguena, M.P., Vindel Cañas, M.P.: Problemes de matemàtica discreta. Universitat Jaume I, 1997

[Gall] Gallier, J.: Discrete Mathematics. Springer, 2011

[Ham] Hamilton, A.G.: Logic for mathematicians, Cambridge U.P. 1978

[LiPi] Lidl, R., Pilz, G.: Applied Abstract Algebra. Second edition. Springer, 1998

[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3. ed. McGraw Hill, 2007

[Rios] Ríos, S.: Matemática finita. Paraninfo, 1974

[Smull] Smullyan, R.M.: A Beginner's guide to Mathematical Logic. Dover, 2014

[Wall2] Wallis, W.D.: A beginner's guide to discrete mathematics. Second edition. Birkhäuser, 2012

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Capítulo 11.
Estructuras algebraicas

Los primeros capítulos del curso tratan los conjuntos y las aplicaciones entre ellos. En este capítulo veremos en general cómo las aplicaciones definen operaciones sobre conjuntos y cuán útil es esta idea. Ya se han visto ejemplos concretos de este hecho, como los espacios vectoriales y las álgebras de Boole.

Tomemos por ejemplo $\mathbb{N}$. Sabemos que los naturales se pueden sumar entre ellos, y el resultado vuelve a ser un número natural. La suma de números naturales la entendemos, pues, como una aplicación $\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ que a cada par de naturales (m,n) le asigna el natural $+(m,n) =: m+n$. En general, dado un conjunto M, aplicaciones de la forma $M\times M\to M$ se llaman *leyes de composición* sobre M.

Además la suma usual sobre $\mathbb{N}$ cumple algunas propiedades, en principio obvias para nosotros: dados tres números naturales da igual cómo se agrupen al sumarlos, el resultado es el mismo (propiedad asociativa de la suma en $\mathbb{N}$); es igual en qué orden se sumen dos números naturales cualesquiera, el resultado no varía (propiedad conmutativa).

Esto significa que la suma dota al conjunto $\mathbb{N}$ de una cierta estructura algebraica. Según qué propiedades cumpla y cuántas leyes de composición involucre recibe uno u otro nombre. En el ejemplo que mencionamos hay una sola ley de composición (la suma) que cumple las propiedades asociativa y conmutativa; se dice que el par $(\mathbb{N},+)$ *posee estructura de* semigrupo conmutativo o, abreviando, que $(\mathbb{N},+)$ *es* un semigrupo conmutativo.

Obviamente no se ha inventado este nombre solamente para $\mathbb{N}$, existen otros muchos conjuntos sobre los que distintas leyes de composición definen la estructura de semigrupo. Por eso ha de definirse en general:

Definición. Sean $M\neq\varnothing$ un conjunto y $\oplus$ una ley de composición sobre M, i.e.

(M0) para cualesquiera $a,b\in M$ se tiene que $a\oplus b\in M$;

si esta ley cumple la propiedad asociativa, es decir, que

(M1) $(a\oplus b)\oplus c = a\oplus(b\oplus c)$ para cualesquiera $a,b,c\in M$

entonces se dice que $\oplus$ dota a M de la estructura de *semigrupo* (o que el par $(M,\oplus)$ es un semigrupo). Si además

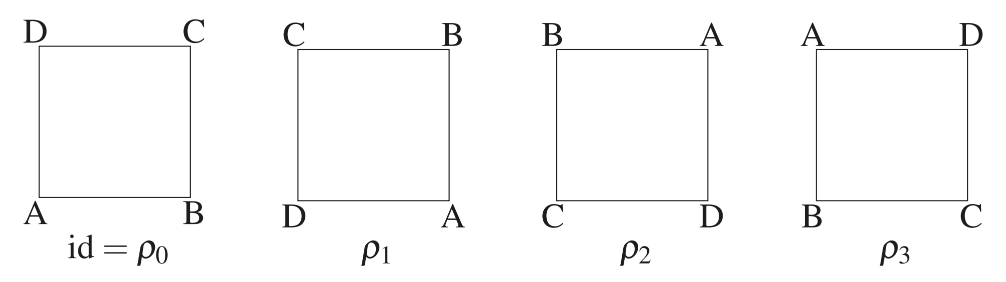
(M2) Para todo $a\in M$ existe un $e\in M$ con $a\oplus e = e\oplus a = a$,

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

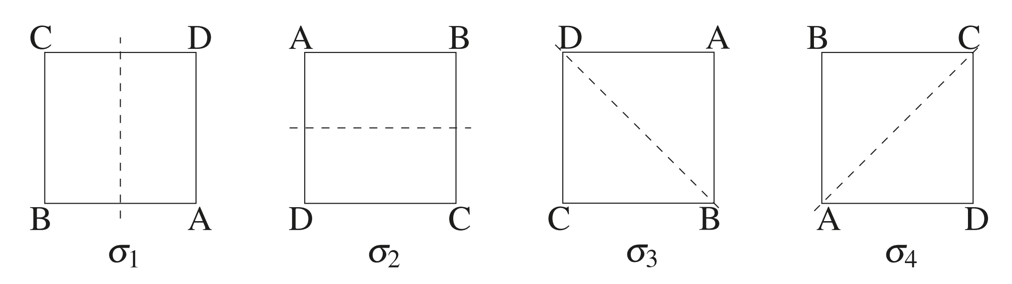
entonces $(M, \oplus)$ es un *monoide*; el elemento e de (M2) se denomina *elemento neutro* respecto de $\oplus$.

Así, el par $(\mathbb{N}, +)$ de los números naturales con la adición usual posee estructura no sólo de semigrupo, sino incluso de monoide (la suma de naturales es obviamente asociativa, y el elemento neutro es 0). Un monoide o un semigrupo $(M, \circ)$ se dice *conmutativo* si para todos $a, b \in M$ se cumple que $a \circ b = b \circ a$.

A veces, las estructuras algebraicas surgen de forma insospechada. Tomemos un *cuadrado* de vértices A, B, C, D, y consideremos los movimientos de este cuadrado que lo dejan fijo (es decir, transformaciones sobre el cuadrado que lo dejan en la misma posición en la que está). Hay ocho, a saber: cuatro giros



que son la identidad o giro de 0°, que denotaremos $\rho_0 = \text{id}$, el giro ρ_1 de 90°, el giro ρ_2 de 180° y el giro ρ_3 de 270°; y también las simetrías $\sigma_1, \sigma_2, \sigma_3$ y σ_4 respecto a los cuatro ejes como en la figura:



Estos movimientos se pueden componer: por ejemplo, la composición $\sigma_2 \circ \sigma_1$ es el resultado de aplicar sucesivamente la simetría σ_1 primero, y la simetría σ_2 después. Y se observa que produce sobre el cuadrado el mismo efecto que aplicar el giro ρ_2. Esquemáticamente, podemos asociar el movimiento σ_1 a una "matriz"

$$\begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$$

que indica que, respecto de la posición inicial de vértices, lleva el vértice B a donde estaba el A, el A a donde estaba el B, etc. Si σ_2 es representado por la "matriz"

$$\begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix},$$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

entonces la composición $\sigma_2 \circ \sigma_1$ se deduce según el esquema

$$\begin{array}{cccc} A & B & C & D \\ B & A & D & C \\ C & D & A & B \end{array}$$

es decir, corresponde al movimiento ρ_2

$$\begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}.$$

(Nótese que en realidad esta escritura con "matrices" expresa con claridad una reordenación del conjunto de vértices: efectivamente, cada uno de los movimientos se puede ver como una biyección del conjunto de vértices $\{A,B,C,D\}$ en sí mismo: es lo que se llama una *permutación* del conjunto $\{A,B,C,D\}$. En este sentido, la "composición de movimientos" es "composición de permutaciones", y el uso de la palabra "composición" para los movimientos queda así justificado. El capítulo 15 proporciona más información sobre permutaciones).

Haciendo lo mismo para cada dos cualesquiera de los ocho movimientos se obtiene una tabla 8×8 con 64 entradas:

$\circ$	id	ρ_1	ρ_2	ρ_3	σ_1	σ_2	σ_3	σ_4
id	id	ρ_1	ρ_2	ρ_3	σ_1	σ_2	σ_3	σ_4
ρ_1	ρ_1	ρ_2	ρ_3	id	σ_4	σ_3	σ_1	σ_2
ρ_2	ρ_2	ρ_3	id	ρ_1	σ_2	σ_1	σ_4	σ_3
ρ_3	ρ_3	id	ρ_1	ρ_2	σ_3	σ_4	σ_2	σ_1
σ_1	σ_1	σ_3	σ_2	σ_4	id	ρ_2	ρ_1	ρ_3
σ_2	σ_2	σ_4	σ_1	σ_3	ρ_2	id	ρ_3	ρ_1
σ_3	σ_3	σ_2	σ_4	σ_1	ρ_3	ρ_1	id	ρ_2
σ_4	σ_4	σ_1	σ_3	σ_2	ρ_1	ρ_3	ρ_2	id

Una tabla así, que recoge (define, de hecho) la operación binaria de una cierta estructura algebraica definida sobre un conjunto finito se denomina *tabla de Cayley*.[1]

Convengamos que la tabla se lee de manera que $\sigma_1 \circ \rho_3 = \sigma_4$, es decir, si se realiza primero ρ_3 y después σ_1 resulta σ_4. Obsérvese que este convenio es relevante, pues $\rho_3 \circ \sigma_1 = \sigma_3$, es decir, la operación "$\circ$" no es conmutativa. Una simple inspección revela los siguientes hechos:

(a) la composición de dos movimientos cualesquiera es de nuevo un movimiento (es decir, no nos encontramos algo diferente a los 8 movimientos que tenemos al componer dos cualesquiera de ellos).

[1]En honor al matemático británico Arthur CAYLEY (1821–1895).

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

(b) Dados tres movimientos x, y, z de los ocho, es igual cómo se agrupen al efectuar la composición de los tres, el resultado es el mismo. Por ejemplo, por un lado se tiene

$$\sigma_3 \circ (\sigma_4 \circ \rho_1) = \sigma_3 \circ \sigma_1 = \rho_3$$

y por otro es

$$(\sigma_3 \circ \sigma_4) \circ \rho_1 = \rho_2 \circ \rho_1 = \rho_3,$$

y esto para cualesquiera tres que tomemos.

(c) Existe un movimiento tal que deja invariante cualquier movimiento que se componga con él (por la izquierda o por la derecha): es la identidad, o sea, el giro de 0 grados.

(d) Dado cualquier movimiento de los ocho, existe otro que al componerlo con él resulta la identidad (se ve en la tabla claramente, pues en cada columna —y en cada fila— aparece una vez la identidad).

Que el conjunto $\mathscr{M} := \{\mathrm{id} = \rho_0, \rho_1, \rho_2, \rho_3, \sigma_1, \sigma_2, \sigma_3, \sigma_4\}$, junto con la composición $\circ$ de movimientos, verifique estas cuatro propiedades se expresa diciendo que $\mathscr{M}$ tiene estructura de grupo respecto de la composición $\circ$. Abstrayendo este fenómeno se obtiene la definición de *grupo*:

Definición. Sean $G \neq \varnothing$ un conjunto, y $* : G \times G \to G$ una ley de composición interna sobre G. El par $(G, *)$ recibe el nombre de *grupo* si verifica las propiedades siguientes:

(G0) Para todo $g, h \in G$ se verifica que efectivamente $g * h \in G$, es decir, la operación $*$ es cerrada en G. (En realidad, tomar esto como axioma de grupo es redundante, pues está implícito en el concepto de ley de "composición".)

(G1) (Propiedad asociativa.) Para todos $g, h, k \in G$ se verifica que

$$(g * h) * k = g * (h * k).$$

(G2) (Existencia de elemento neutro.) Existe un $e \in G$ tal que

$$g * e = e * g = g \quad \text{para todo } g \in G.$$

Este elemento $e \in G$ se llama *elemento neutro* de $(G, *)$. A veces se codifica en la notación de grupo y se escribe $(G, *, e)$.

(G3) (Todo elemento tiene inverso.) Para cualquier $g \in G$ existe un elemento $h \in G$ tal que

$$g * h = h * g = e.$$

El elemento h se llama *inverso* de g.

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

Dicho de otra manera, un grupo es un monoide en el que todo elemento tiene inverso.

Ejemplos. (a) El grupo de movimientos $(\mathscr{M},\circ)$ del cuadrado visto anteriormente es un grupo, con elemento neutro el giro $\mathrm{id}=\rho_0$ de 0 grados.

(b) Los pares $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{Q}\setminus\{0\},\cdot)$, $(\mathbb{R}\setminus\{0\},\cdot)$ son todos grupos, donde $+$ y $\cdot$ denotan la suma y el producto usual, respectivamente; el elemento neutro de los que tienen a la suma como ley de composición es el 0, y el de los que tienen al producto es el 1.

(c) El par $(\mathbb{Q},\cdot)$ no es un grupo, pues *no todo* elemento de $\mathbb{Q}$ posee inverso respecto del producto: ¡el 0 no lo tiene!

En la tabla anterior la identidad aparecía en cada columna o fila una sola vez, ya que: dado un elemento g de un grupo $(G,*,e)$, su inverso es único; en efecto, supongamos que $g\in G$ tuviera dos inversos $h_1,h_2\in G$, entonces coinciden:

$$h_1 \overset{(G2)}{=} h_1*e \overset{(G3)}{=} h_1*(g*h_2) \overset{(G1)}{=} (h_1*g)*h_2 \overset{(G3)}{=} e*h_2 \overset{(G2)}{=} h_2.$$

Como el inverso de un elemento g de un grupo es único, podemos dedicarle una notación que muestre su dependencia (unívoca) de g. Se suele escribir g^{-1} o $1/g$, en lo que se llama *notación multiplicativa*. Si la ley de composición que tiene es la suma se suele emplear la *notación aditiva*, y así se dirá que el inverso de un elemento a del grupo es $-a$. Así, el inverso de 4 en $(\mathbb{Z},+)$ se denota -4, pero el inverso de 4 en $(\mathbb{Q}\setminus\{0\},\cdot)$ se escribe $1/4$ ó 4^{-1}.

Observamos que no se exige que la ley de composición de un grupo sea conmutativa. Cuando esto ocurre se otorga al grupo un apellido especial:

Definición. Sea $(G,*)$ un grupo en el que se verifica la propiedad conmutativa, es decir, que para todos los elementos $g,h\in G$

$$g*h=h*g.$$

Entonces el grupo se dice *abeliano*.

Ejemplo. Los grupos de (b) en el ejemplo anterior son todos abelianos; en cambio, el grupo de los movimientos $(\mathscr{M},\circ)$ del cuadrado no lo es: por ejemplo

$$\sigma_1\circ\rho_3=\sigma_3\neq\sigma_4=\rho_3\circ\sigma_1.$$

A menudo se dice que el álgebra es el arte de resolver ecuaciones. En este sentido:

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Teorema 11.1. *Sea $(G,*)$ un grupo. Entonces para cualesquiera $a,b \in G$, las ecuaciones*

$$a*x=b, \quad y*a=b$$

poseen una única solución en G.

Demostración. Sea e el elemento neutro de G. Basta tomar el producto por a^{-1} por la izquierda en la primera ecuación, y se obtiene

$$a^{-1}*(a*x)=a^{-1}*b \Leftrightarrow (a^{-1}*a)*x=a^{-1}*b \Leftrightarrow e*x=a^{-1}*b \Leftrightarrow x=a^{-1}*b.$$

Análogamente, multiplicando por a^{-1} por la derecha en la segunda ecuación se obtiene:

$$(y*a)*a^{-1}=b*a^{-1} \Leftrightarrow y*(a*a^{-1})=b*a^{-1} \Leftrightarrow y*e*x=b*a^{-1} \Leftrightarrow y=b*a^{-1}.$$

(Obsérvese que si el grupo no es abeliano, multiplicar por la derecha o por la izquierda no es lo mismo). La unicidad se sigue de la unicidad del inverso. □

En la construcción de los sistemas de números $(\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\ldots)$, la voluntad de resolver ecuaciones de un determinado tipo ha desempeñado históricamente un papel esencial. De esta manera se puede explicar, por ejemplo, el paso de $\mathbb{N}$ a $\mathbb{Z}$, al querer resolver ecuaciones del tipo

$$a+x=b, \quad a,b \in \mathbb{N};$$

o también el paso de $\mathbb{Z}$ a $\mathbb{Q}$, con ecuaciones del tipo

$$a \cdot x=b, \quad a,b \in \mathbb{Z},\ a \neq 0.$$

Existen, empero, estructuras algebraicas más "complejas" que la de grupo.

Definición. Sea $A \neq \varnothing$ un conjunto, y sean $+: A \times A \to A$, $\cdot : A \times A \to A$ dos leyes de composición sobre A. Se dice que $(A,+,\cdot)$ es un anillo[2] si se cumple que:

(A0) (Clausura de las leyes:) Para todos $a,b \in A$ es $a+b \in A$ así como $a \cdot b \in A$.
(A1) (Asociatividad de "$+$":) $\forall a,b,c \in A$ se tiene $(a+b)+c=a+(b+c)$.
(A2) (Conmutatividad de "$+$":) $\forall a,b \in A$ se tiene $a+b=b+a$.
(A3) (Existencia de elemento neutro para "$+$":) Existe un elemento $\vartheta \in A$ tal que $\vartheta+a=a$ para todo $a \in A$.
(A4) (Todo elemento tiene inverso aditivo:) Para cualquier elemento $a \in A$ existe un elemento $b \in A$ tal que $a+b=\vartheta$.
(A5) (Asociatividad de "$\cdot$":) $\forall a,b,c \in A$ se tiene $(a \cdot b) \cdot c=a \cdot (b \cdot c)$.

[2]Técnicamente esta definición es la de anillo *conmutativo* y *con unidad*: conmutativo porque el producto es conmutativo; y con unidad porque existe elemento neutro multiplicativo.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

(A6) (Conmutatividad de " $\cdot$":) $\forall a, b \in A$ se tiene $a \cdot b = b \cdot a$.
(A7) (Existencia de elemento unidad:) Existe un $\xi \in A$ tal que para todo $a \in A$ se cumple que $\xi \cdot a = a$.
(A8) (Propiedad distributiva:) $\forall a, b, c \in A$ se tiene $a \cdot (b + c) = a \cdot b + a \cdot c$.

Obsérvese que —junto con (A0)— los axiomas (A1)–(A4) se pueden resumir diciendo que $(A, +)$ es grupo abeliano y los axiomas (A5)–(A7) diciendo que $(A, \cdot)$ es monoide conmutativo. Por comodidad escribiremos *ab* en lugar de $a \cdot b$. También se suelen emplear los símbolos genéricos $0 = 0_R$ para el elemento neutro de la operación "+" (en vez de ϑ) y $1 = 1_R$ para el elemento neutro de la operación "·" (en lugar de ξ). No se exige $0 \neq 1$, y así el menor conjunto posible al que se puede dotar de estructura de anillo es el anillo cero $\{0\}$; de hecho, $0 = 1$ si y solamente si $A = \{0\}$.

Ejemplo. El ejemplo más cercano es el anillo $(\mathbb{Z}, +, \cdot)$ de los números enteros, con 0 el elemento neutro de la suma y 1 la unidad del axioma (A7). El anillo de polinomios $\mathbb{R}[X]$ con coeficientes en $\mathbb{R}$ en la indeterminada X, junto con la adición y la multiplicación usuales, tiene también estructura de anillo.

A la vista de la definición de anillo, destaca la ausencia de una propiedad análoga a (A4) para el producto:

Definición. Un anillo K se llama *cuerpo* si todo elemento $\neq \vartheta$ posee inverso en K respecto de "·"; es decir, si

(K) Para cualquier $a \in K \setminus \{\vartheta\}$ existe un elemento $b \in K$ tal que $a \cdot b = \xi$;

Ejemplos de cuerpo son, respecto de las operaciones usuales, los números racionales $(\mathbb{Q}, +, \cdot)$, los números reales $(\mathbb{R}, +, \cdot)$, o el cuerpo de los números complejos $(\mathbb{C}, +, \cdot)$. El menor conjunto al que se puede dotar de estructura de cuerpo ha de contener dos elementos, que por la axiomática han de ser necesariamente ϑ y ξ. Es un ejercicio comprobar que las dos tablas siguientes definen operaciones $+$ y $\cdot$ sobre el conjunto $\{\vartheta, \xi\}$ que le dotan de estructura de cuerpo:

$+$	ϑ	ξ
ϑ	ϑ	ξ
ξ	ξ	ϑ

$\cdot$	ϑ	ξ
ϑ	ϑ	ϑ
ξ	ϑ	ξ

El cuerpo $(\{\vartheta, \xi\}, +, \cdot)$ se suele denotar por $\mathbb{F}_2$ y se llama el *cuerpo finito de dos elementos*. Es también habitual emplear la notación 0 y 1 para ϑ y ξ, respectivamente.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Homomorfismos. Una estructura algebraica siempre lleva asociada un tipo de aplicaciones que respetan sus operaciones definitorias. Así por ejemplo, del álgebra lineal conocemos las aplicaciones lineales entre espacios vectoriales. Sucede lo análogo en el caso de la estructura de grupo o la de anillo, como veremos para concluir el capítulo. Empleando la notación multiplicativa, se tiene:

Definición. Sea $(G,*)$ un grupo con elemento neutro 1_G y sea $(H,\circ)$ un grupo con elemento neutro 1_H. Una aplicación $f : G \to H$ se denomina *homomorfismo de grupos* si para cualesquiera $a,b \in G$ se cumple que

(a) $f(a*b) = f(a) \circ f(b)$;
(b) $f(1_G) = 1_H$.

Normalmente, por economía de símbolos, las operaciones en el grupo de partida y en el de llegada se denotan igual. Para un homomorfismo de grupos $f : G \to H$ se define su *núcleo* como

$$\mathrm{Ker}(f) := \{g \in G : f(g) = 1_H\}.$$

El núcleo de un homomorfismo de grupos permite caracterizar fácilmente aquellos homomorfismos que son inyectivos:

Teorema 11.2. *Un homomorfismo de grupos $f : G \to H$ es inyectivo si y solamente si* $\mathrm{Ker}(f) = \{1_G\}$.

La prueba de este resultado es un mero ejercicio.

La estructura de anillo (y de cuerpo, pues su definición es similar) también tiene sus homomorfismos:

Definición. Sean $(R,+,\cdot)$ y $(R',+',\cdot')$ dos anillos. Una aplicación $\varphi : R \to R'$ se denomina *homomorfismo de anillos* si para todos $a,b \in R$ se verifica

(a) $\varphi(a+b) = \varphi(a) +' \varphi(b)$;
(b) $\varphi(a \cdot b) = \varphi(a) \cdot' \varphi(b)$;
(c) $\varphi(1_R) = 1_{R'}$.

Si el homomorfismo es biyectivo se denomina *isomorfismo*. Un anillo R se dice *isomorfo* a otro R', y se escribe $R \cong R'$, si se puede establecer un isomorfismo entre ellos.

Es obvio que si $\varphi : R \to R'$ es un homomorfismo de anillos, en particular φ es un homomorfismo del grupo $(R,+)$ en el grupo $(R',+')$; de ello se deduce por

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

ejemplo que $\varphi(0_R) = 0_{R'}$ y que φ es una aplicación inyectiva si y solamente si $\mathrm{Ker}(\varphi) = \{0_R\}$. (Efectivamente, también el concepto de núcleo admite ser definido en el contexto de los homomorfismos de anillos). Como aplicación, demostremos el resultado siguiente:

Teorema 11.3. *Sea* $(K,+,\cdot)$ *un cuerpo, y sea* $(R',+',\cdot')$ *un anillo tal que* $R' \neq \{0_{R'}\}$. *Todo homomorfismo de anillos* $\varphi : K \to R'$ *es inyectivo.*

Demostración. Basta demostrar que $\mathrm{Ker}(\varphi) = \{0_K\}$. Supongamos lo contrario, es decir, supongamos que existe $a \in K$, $a \neq 0_K$, tal que $\varphi(a) = 0_{R'}$. Al ser $a \in K \setminus \{0_K\}$, posee inverso multiplicativo a^{-1}, y entonces se verifica que

$$0_{R'} = 0_{R'} \cdot' \varphi(a^{-1}) = \varphi(a) \cdot' \varphi(a^{-1}) = \varphi(a \cdot a^{-1}) = \varphi(1_K) = 1_{R'},$$

lo que contradice la hipótesis $R' \neq \{0_{R'}\}$. □

Como consecuencia se verifica que todo homomorfismo de cuerpos es inyectivo.

El capítulo siguiente será dedicado al estudio de una estructura algebraica relevante y en realidad conocida: el anillo de los números enteros; no sin antes estudiar su base definitoria, el conjunto de los números naturales.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

[Ant] Antoine, R., Camps, R., Moncasi, J.: Introducció a l'àlgebra abstracta. Universitat Autònoma de Barcelona, 2007

[Art] Artin, M.: Algebra. Birkhäuser, Basel 1993

[BRV] Basart, J. M., Rifà, J., Villanueva, M.: Fonaments de matemàtica discreta. Elements de combinatòria i d'aritmètica. Universitat Autònoma de Barcelona, 1999

[Big] Biggs, N.L.: Discrete Mathematics. Second ed. Oxford U.P., 2004

[FG] Ferrando, J.C., Gregori, V.: Matemática Discreta. 2. ed. Reverté, 2002

[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3. ed. McGraw Hill, 2007

[SchWie] Schafmeister, O., Wiebe, H.: Grundzüge der Algebra. B.G. Teubner, 1978

Capítulo 12. Aritmética de los números naturales y enteros

Los números naturales forman el conjunto numérico más sencillo que manejamos; dotados de la adición, poseen una estructura sencilla, como es la de monoide conmutativo. Otra propiedad, ya comentada en el capítulo 4, es que el conjunto $\mathbb{N}$ admite un orden total, con el que estamos familiarizados desde el colegio:

$$0 < 1 < 2 < 3 < \cdots < n < \cdots < \cdots$$

Este conjunto $\mathbb{N}$ así ordenado posee una propiedad más, tan sencilla como importante: todo subconjunto no vacío de $\mathbb{N}$ posee un elemento mínimo respecto del orden $\leq$. A esto nos referimos diciendo que el orden $\leq$ sobre el conjunto $\mathbb{N}$ es un *buen orden*. Esta propiedad es consustancial a la naturaleza de los números naturales, que podemos definir de la manera siguiente:

Definición. Por conjunto de los *números naturales* entendemos un monoide $(\mathbb{N},+)$ tal que:

(a) La operación $+$ es conmutativa, con elemento neutro 0 y con al menos otro elemento distinto del neutro.

(b) Todo elemento es cancelable, es decir, para cualesquiera $a,x,y \in \mathbb{N}$ se verifica que

$$ax = ay \implies x = y,$$

pero solamente el 0 posee inverso.

(c) *Axioma del elemento mínimo*: todo subconjunto no vacío $M \subseteq \mathbb{N}$ posee un elemento mínimo m en el sentido siguiente: para todo $n \in M$ existe $x \in \mathbb{N}$ con $m + x = n$.

A partir de esta definición se pueden deducir todas las propiedades sobre números naturales que conocemos, por ejemplo las relativas al orden. Definamos, para comenzar, el orden en $\mathbb{N}$: para todo $m,n \in \mathbb{N}$

$$m \leq n \;:\Longleftrightarrow\; \text{existe } x \in \mathbb{N} \text{ con } m + x = n.$$

ISBN: 978-84-17900-65-6

DOI: http://dx.doi.org/10.6035/Sapientia170

Se puede probar a partir de esta definición que $\leq$ es un orden total para el conjunto de los números naturales. El elemento mínimo de $\mathbb{N}$ es el 0, pues para todo $n \in \mathbb{N}$ es $0+n=n$, es decir, $0 \leq n$. El conjunto $\mathbb{N} \setminus \{0\}$ también posee un mínimo, por el axioma del elemento mínimo, que denotaremos por 1. Con las notaciones usuales para las relaciones de orden vistas en el capítulo 4 se pueden probar las propiedades siguientes:

Teorema 12.1. *Sean $m,n,p \in \mathbb{N}$.*

(1) *Se verifica que $m \leq n \implies m+p \leq n+p$, y también que $m < n \implies m+p < n+p$.*
(2) *$m < n$ si y solamente si existe $x \in \mathbb{N}$, $x \neq 0$, tal que $m+x=n$; en particular, $m < m+1$.*
(3) *De $m < n$ se sigue $m+1 \leq n$.*
(4) *Si $n \neq 0$, existe un único $x \in \mathbb{N}$ tal que $x+1=n$.*

De estas propiedades destacamos que para cualquier $m \in \mathbb{N}$ es $m < m+1$ y que para cualquier natural n tal que $m < n \leq m+1$ se verifica que $m+1 \leq n$ y por tanto, $n = m+1$. Este natural $m+1$ es, por así decir, el siguiente mayor que m respecto del orden $\leq$, y se le llama *sucesor* de m.

La noción de sucesor junto con el axioma del elemento mínimo nos permiten probar otro resultado fundamental relativo a los números naturales que ya tratamos en el capítulo 2, aunque allí solamente desde un punto de vista meramente instrumental:

Teorema 12.2 (Principio de inducción)**.** *Sea M un subconjunto de $\mathbb{N}$ para el que*

1. *$0 \in M$;*
2. *para cualquier $n \in M$ también $n+1 \in M$.*

Entonces $M = \mathbb{N}$.

Demostración. Razonemos por reducción al absurdo y supongamos que $M \neq \mathbb{N}$, entonces $\mathbb{N} \setminus M \neq \varnothing$ y por tanto, el conjunto $\mathbb{N} \setminus M$ posee un elemento mínimo m. Como $0 \in M$, i.e., $0 \notin \mathbb{N} \setminus M$, entonces $m \neq 0$. Por el Teorema 12.1(4), existe $x \in \mathbb{N}$ tal que $m = x+1$. Entonces es $x < m$ y por la minimalidad de m en $\mathbb{N} \setminus M$, el elemento x no puede pertenecer a $\mathbb{N} \setminus M$, lo que significa que $x \in M$. Por hipótesis, también $x+1 \in M$, luego $m \in M$, lo que contradice la pertenencia $m \in \mathbb{N} \setminus M$.

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

La formulación usual del principio de inducción es la vista en el capítulo 2, aunque admite varias formulaciones, como la que acabamos de exponer.

A partir de los números naturales se pueden construir los númerios enteros: la construcción formal de $\mathbb{Z}$ a partir de $\mathbb{N}$ está explicada en el capítulo 5 (requerimos para ello la noción de relación de equivalencia). También sabemos que las operaciones $+$ y $\cdot$ usuales dotan a $\mathbb{Z}$ de la estructura de anillo conmutativo. El siguiente teorema, que no demostraremos,[1] es conocido también desde la escuela:

Teorema 12.3 (Teorema fundamental de la aritmética)**.** *Cualquier número entero z descompone como producto finito*

$$z = u \cdot p_1^{e_1} \cdots p_s^{e_s},$$

donde $u \in \{-1, 1\}$, $e_i \in \mathbb{N} \setminus \{0\}$ y los números p_i son números primos tales que $p_i \neq p_j$ si $i \neq j$. Además, esta descomposición en factores primos es única salvo reordenación de los subíndices.

□

Sabemos que $(\mathbb{Z}, +, \cdot)$ es un anillo, pero no es cuerpo, pues no todo elemento tiene un inverso multiplicativo: solamente lo tienen 1 y -1. Este hecho impide que la división por cualquier número distinto de 1 y de -1 sea una operación cerrada (una ley de composición interna) en $\mathbb{Z}$. Por ejemplo, 2 tiene inverso aditivo en $\mathbb{Z}$, el -2, pero no un inverso multiplicativo: si lo tuviera, habría de ser $1/2$, pero ¡este número no es entero! Lo que se verifica es el teorema de división, conocido desde el colegio:

Teorema 12.4 (División con resto)**.** *Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Entonces existen únicos $q, r \in \mathbb{Z}$ tales que*

$$a = q \cdot b + r \quad \text{y } r = 0 \text{ ó } 0 < r < |b|.$$

Demostración. Sin pérdida de generalidad podemos suponer $a, b \in \mathbb{N}$, y por tanto, $q, r \in \mathbb{N}$. Basta entonces observar que cualquier $a \in \mathbb{Z}$ es o bien un múltiplo de b, esto es, $a = bq$, o bien está entre dos múltiplos consecutivos de b

$$bq < a < b(q+1) = bq + b.$$

En el primer caso es $r = 0$; en el segundo caso, de la desigualdad izquierda resulta $a - bq = r > 0$, y la de la derecha ofrece $a - bq = r < b$, con lo que $0 < r < b$. □

[1] En realidad su demostración usa propiedades que veremos unos párrafos después, pero por conveniencia de la exposición lo presentamos aquí.

ISBN: 978-84-17900-65-6

DOI: http://dx.doi.org/10.6035/Sapientia170

Si $r = 0$ en la expresión del teorema diremos que a es divisible por b, o que b es un divisor de a, o que a es un múltiplo de b, o que b divide a a. Se escribirá $b|a$ y en caso contrario, $b \nmid a$.

Ejemplo. (i) Sean $a = 15$, $b = 5$. En este caso 15 es divisible por 5, ya que $15 = 3 \cdot 5 + 0$ (es decir, en la notación del teorema $q = 3$ y $r = 0$). Así, $5 \mid 15$.
(ii) Sean $a = 15$, $b = -4$. En este caso $15 = (-3) \cdot (-4) + 3$, es decir, $q = -3$ y $r = 3$; por tanto, $-4 \nmid 15$ y se cumple que

$$|r| = |3| = 3 < 4 = |-4| = |b|.$$

Un número entero d se llama *divisor común* de $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ si d divide a todos los a_i, es decir, si para cada $i = 1, \ldots, n$ existe $b_i \in \mathbb{Z}$ tal que $a_i = b_i \cdot d$. Un número entero v se llama *múltiplo común* de $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ si v es un múltiplo de todos los a_i, es decir, si para cada $i = 1, \ldots, n$ existe $c_i \in \mathbb{Z}$ tal que $v = c_i \cdot a_i$.

Ejemplo. (i) Sean los números enteros $6, 12, 144$. El 2 es un divisor común a 6, 12 y 144, así como $-2, 3, -3, 6$ y -6, y por supuesto 1 y -1.
(ii) Sean los números enteros $2, 4, 12$. Un múltiplo común a 2, 4 y 12 es 12, pero también -12 y, en general, cada uno de la forma $12 \cdot \lambda$ con $\lambda \in \mathbb{Z}$.

Definición. (a) Los números $a_1, \ldots, a_n \in \mathbb{Z}$ se llaman *primos entre sí* o *coprimos* si los únicos divisores comunes de $a_1, \ldots, a_n$ son 1 y -1.
(b) Se llama *máximo común divisor* de $a_1, \ldots, a_n$ al mayor entero positivo d de entre los divisores comunes de $a_1, \ldots, a_n$. Escribiremos $d = \mathrm{mcd}(a_1, \ldots, a_n)$.
(c) Se llama *mínimo común múltiplo* de $a_1, \ldots, a_n$ al menor entero positivo v de entre los múltiplos comunes de $a_1, \ldots, a_n$. Escribiremos $v = \mathrm{mcm}(a_1, \ldots, a_n)$.

Ejemplo. Los enteros 3, 5 y 9 son primos entre sí, aunque no son *dos a dos* primos entre sí. Siguiendo con los números del ejemplo anterior, $\mathrm{mcd}(6, 12, 144) = 6$ y $\mathrm{mcm}(2, 4, 12) = 12$.

El cálculo del máximo común divisor para números muy grandes sería tedioso de no ser por un método eficiente llamado “algoritmo de Euclides”. Este algoritmo se basa en que, a partir de toda igualdad de la forma

$$a = bq + r$$

se puede deducir que

$$\mathrm{mcd}(a, b) \overset{(*)}{=} \mathrm{mcd}(b, r).$$

¿Por qué? Sea u un divisor común de a y b, es decir,

$$a = su, \; b = tu \;\text{ con } s, t \in \mathbb{Z}$$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

entonces también es un divisor de r, ya que

$$r = a - bq = su - tuq = (s - tq)u.$$

Recíprocamente, todo divisor v común a b y r, es decir

$$b = s'v, \ r = t'v \ \text{ con } \ s', t' \in \mathbb{Z}$$

ha de serlo también de a, pues

$$a = bq + r = s'vq + t'r = (s'q + t')v.$$

Por ello, *todo* divisor común de a y b también es un divisor común de b y r, y al revés.

Si, por ello, el conjunto de *todos* los divisores comunes de a y b es idéntico al conjunto de todos los divisores comunes a b y r, ha de cumplirse en particular que el máximo común divisor de a y b es igual al máximo común divisor de b y r, como queríamos.

Teorema 12.5. *Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Denotemos $r_0 := b$. Entonces existe un número finito de divisiones sucesivas*

$$\begin{array}{lcll} a & = & q_1 \cdot r_0 & + \ r_1 \\ r_0 & = & q_2 \cdot r_1 & + \ r_2 \\ r_1 & = & q_3 \cdot r_2 & + \ r_3 \\ & \vdots & & \\ r_{n-2} & = & q_n \cdot r_{n-1} & + \ r_n \\ r_{n-1} & = & q_{n+1} \cdot r_n & + \ r_{n+1} \end{array}$$

con $r_{n+1} = 0$ y $|r_n| = \mathrm{mcd}(a, b)$.

Demostración. Este proceso es finito: ha de concluir tras a lo sumo b pasos, pues

$$b > r_1 > r_2 > \cdots > 0$$

es una sucesión estrictamente decreciente de enteros positivos. La igualdad $\mathrm{mcd}(a, b) = r_n$ se deduce de la aplicación reiterada de la igualdad $(*)$ vista varias líneas arriba en las sucesivas divisiones: en efecto,

$$\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r_1) = \mathrm{mcd}(r_1, r_2) = \cdots = \mathrm{mcd}(r_{n-1}, r_n) = \mathrm{mcd}(r_n, 0) = r_n.$$

□

El algoritmo de Euclides nos ofrece el cálculo efectivo del máximo común divisor de dos números enteros. El cálculo del máximo común divisor y del mínimo común múltiplo de varios enteros se puede reducir al cálculo para dos enteros; además el cálculo del mínimo común múltiplo de dos números enteros se reduce a

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

su vez al cálculo de su máximo común divisor. Estas y otras propiedades importantes quedan recogidas en el resultado siguiente (cuya prueba omitimos):

Teorema 12.6. *Sean $a,b,c,g \in \mathbb{Z}$ con $g \geq 0$. Se verifica:*

(1) *Si a,b son primos entre sí entonces* $\mathrm{mcd}(a,b) = 1$ *y* $\mathrm{mcm}(a,b) = |a \cdot b|$.
(2) $\mathrm{mcd}(a,b) \cdot \mathrm{mcm}(a,b) = |a \cdot b|$.
(3) *Existen $c,d \in \mathbb{Z}$ tales que $a = c \cdot \mathrm{mcd}(a,b)$, $b = d \cdot \mathrm{mcd}(a,b)$, donde c y d son primos entre sí.*
(4) $\mathrm{mcm}(ga,gb) = g \cdot \mathrm{mcm}(a,b)$.
(5) $\mathrm{mcd}(a,b,c) = \mathrm{mcd}(a,\mathrm{mcd}(b,c))$.
(6) $\mathrm{mcm}(a,b,c) = \mathrm{mcm}(a,\mathrm{mcm}(b,c))$.

Del algoritmo de Euclides se deduce la importantísima “identidad de Bézout”:

Teorema 12.7. *(Lema de Bézout) Todo conjunto de números enteros $a_1,\ldots,a_n$ posee máximo común divisor d; este se puede expresar como combinación lineal en $\mathbb{Z}$ de $a_1,\ldots,a_n$, esto es, existen $\alpha_1,\ldots,\alpha_n \in \mathbb{Z}$ tales que*

$$\alpha_1 a_1 + \ldots + \alpha_n a_n = d.$$

Esta igualdad recibe el nombre de identidad de Bézout *en honor al matemático francés Étienne* BÉZOUT *(1730–1783). En particular, si $a_1,\ldots,a_n$ son primos entre sí, existe una escritura del* 1 *en esta forma.*

Demostración. Probemos el resultado para $n = 2$ con $a_1 = a$ y $a_2 = b$; para cualquier n se sigue aplicando el principio de inducción. Considérense las divisiones sucesivas del Teorema 12.5 y sus restos. De la primera división se deduce que

$$r_1 = a - q_1 b$$

de forma que r_1 se puede escribir en la forma $k_1 a + \ell_1 b$ (donde en este caso es $k_1 = 1$ y $\ell_1 = -q_1$). De la siguiente división se sigue que

$$r_2 = b - q_2 r_1 = b - q_2(k_1 a + \ell_1 b) = (-q_2 k_1)a + (1 - q_2 \ell_1)b = k_2 a + \ell_2 b.$$

Obviamente, este proceso se puede continuar para los restos sucesivos hasta conseguir una escritura $r_n = ka + \ell b$ para ciertos $k,\ell \in \mathbb{Z}$, como se quería. □

Existe una versión extendida del algoritmo que permite encontrar los coeficientes de la identidad de Bézout, como se ilustra a continuación:

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Ejemplo. Queremos encontrar la identidad de Bézout para los enteros 30 y 52. Por tanto, aplicamos el algoritmo de Euclides para calcular $\mathrm{mcd}(30,52)$:

$$\begin{array}{lclcl} 52 & = & 1\cdot 30 & + & 22 \\ 30 & = & 1\cdot 22 & + & 8 \\ 22 & = & 2\cdot 8 & + & 6 \\ 8 & = & 1\cdot 6 & + & \mathbf{2} \\ 6 & = & 3\cdot 2 & + & 0 \end{array}$$

y así $\mathrm{mcd}(30,52) = 2$. Deshaciendo el camino andado "con vista" encontramos la identidad de Bézout:

$$\begin{aligned} 2 &= 8-1\cdot 6 = 8-(22-2\cdot 8) = 3\cdot 8-1\cdot 22 \\ &= 3\cdot(30-1\cdot 22)-1\cdot 22 = 3\cdot 30-4\cdot 22 \\ &= 3\cdot 30-4\cdot(52-1\cdot 30) = 3\cdot 30-4\cdot 52+4\cdot 30 \\ &= 7\cdot 30-4\cdot 52. \end{aligned}$$

Restrinjámonos por simplicidad a la identidad de Bézout en dos variables; esta plantea un interrogante: dados tres números $a,b,n \in \mathbb{Z}$, ¿cuándo se pueden encontrar $x,y \in \mathbb{Z}$ tales que $n = a\cdot x + b\cdot y$? Ecuaciones de esta forma se llaman *ecuaciones diofánticas lineales en dos variables*. Los dos teoremas siguientes nos dicen cuándo son resolubles, y cómo es el conjunto de sus soluciones.

Teorema 12.8. *Sean $x_0, y_0 \in \mathbb{Z}$. El par (x_0,y_0) es solución de la ecuación diofántica $ax+by=n$ si y solamente si $\mathrm{mcd}(a,b)|n$. Además, si denotamos $d := \mathrm{mcd}(a,b)$, una solución particular es*

$$\begin{array}{lcl} x_0 & = & \frac{n}{d}\cdot\alpha \\ y_0 & = & \frac{n}{d}\cdot\beta, \end{array}$$

siendo α y β los coeficientes de la identidad de Bézout para d, es decir, enteros tales que $d = \alpha\cdot a + \beta\cdot b$.

Una ecuación diofántica lineal en dos variables resoluble no tiene solamente una, sino que tiene infinitas soluciones:

Teorema 12.9. *Si el par (x_0,y_0) es una solución particular de la ecuación*

$$n = ax+by,$$

entonces todas las soluciones $x,y \in \mathbb{Z}$ de la misma son

$$\begin{array}{lcl} x & = & x_0+\frac{b}{d}\cdot\lambda \\ y & = & y_0-\frac{a}{d}\cdot\lambda, \end{array}$$

para cualquier $\lambda \in \mathbb{Z}$, y donde $d = \mathrm{mcd}(a,b)$.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

[Ant] Antoine, R., Camps, R., Moncasi, J.: Introducció a l'àlgebra abstracta. Universitat Autònoma de Barcelona, 2007

[BRV] Basart, J. M., Rifà, J., Villanueva, M.: Fonaments de matemàtica discreta. Elements de combinatòria i d'aritmètica. Universitat Autònoma de Barcelona, 1999

[Big] Biggs, N.L.: Discrete Mathematics. Second ed. Oxford U.P., 2004

[Cab] Caballero Roldán, Rafael et al.: Matemática Discreta para Informáticos. Ejercicios resueltos. Pearson/Prentice Hall, 2007

[Conr] Conradie, W., Goranko, V.: Logic and Discrete Mathematics. A concise introduction. Wiley, 2015

[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3 ed. McGraw Hill, 2007

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Capítulo 13. Aritmética modular

Imaginemos que estamos sentados tomando un café en una terraza a las 11 de la mañana, y queremos quedar con un amigo para comer dentro de tres horas: le diremos que queremos quedar a las dos. Inconscientemente, hemos identificado el número 14 con el número 2, porque

$$14 = 2 + 12.$$

En otras palabras, hemos dividido 14 entre 12 y hemos tomado el resto de esa división, que es 2. En este capítulo queremos entender este fenómeno en general, es decir, no solamente para 12 sino para cualquier número natural mayor que 1. Para ello, rescatamos la relación “ser congruente con”: sea $m \in \mathbb{Z}$, con $m \geq 2$; para cualesquiera dos enteros a,b se dice que *a es congruente con b módulo m*, y se escribe

$$a \equiv b \mod m$$

si a y b poseen el mismo resto en la división por m, o lo que es lo mismo, si $a-b$ es un mútiplo de m, es decir, si existe $z \in \mathbb{Z}$ tal que $a-b = zm$. Por ejemplo, $14 \equiv 2 \mod 12$, $13 \equiv -2 \mod 3$, $15 \not\equiv 12 \mod 11$.

Como vimos al final del capítulo 5, la relación de congruencia es una relación de equivalencia, y su conjunto cociente es

$$\mathbb{Z}_m := \{[0],[1],\ldots,[m-1]\},$$

donde la clase de equivalencia $[k]$ relativa a un entero $0 \leq k < m$ contiene todos los mútiplos de k. Por ejemplo, para $m = 4$ es

$$\mathbb{Z}_4 = \{[0],[1],[2],[3]\},$$

con

$$\begin{aligned}
[0] &= \{\ldots,-12,-8,-4,0,4,8,12,16,\ldots\} \\
[1] &= \{\ldots,-11,-7,-3,1,5,9,13,17,\ldots\} \\
[2] &= \{\ldots,-10,-6,-2,2,6,10,14,18,\ldots\} \\
[3] &= \{\ldots,-9,-5,-1,3,7,11,15,19,\ldots\}.
\end{aligned}$$

No son difíciles de demostrar los asertos siguientes:

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Teorema 13.1. *Sea $m \in \mathbb{Z}$, $m \geq 2$.*

(a) *Si $a_1 \equiv b_1 \mod m$ y $a_2 \equiv b_2 \mod m$ entonces $a_1 + a_2 \equiv b_1 + b_2 \mod m$.*
(b) *Si $a_1 \equiv b_1 \mod m$, entonces $-a_1 \equiv -b_1 \mod m$.*
(c) *Si $a_1 \equiv b_1 \mod m$ y $a_2 \equiv b_2 \mod m$ entonces $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \mod m$.*

Este buen comportamiento de las congruencias respecto de la suma y el producto en $\mathbb{Z}$ permite definir una suma y producto en el conjunto cociente $\mathbb{Z}_m$ heredadas de aquellas:

$$\begin{array}{ccc} \mathbb{Z}_m \times \mathbb{Z}_m & \longrightarrow & \mathbb{Z}_m \\ ([a],[b]) & \mapsto & [a]+[b] := [a+b] \end{array} \qquad \begin{array}{ccc} \mathbb{Z}_m \times \mathbb{Z}_m & \longrightarrow & \mathbb{Z}_m \\ ([a],[b]) & \mapsto & [a]*[b] := [a \cdot b] \end{array}$$

Nótese que las leyes de composición $+$ y $\cdot$ son las que estamos definiendo aquí, en tanto que las "$+$" y "$\cdot$" que aparecen dentro de los corchetes son las usuales de $\mathbb{Z}$. Como las primeras son heredadas de estas definidas para $\mathbb{Z}$, por simplicidad las denotaremos de igual forma.

Dado un entero $m \geq 2$, es rutinario comprobar que $(\mathbb{Z}_m, +, \cdot)$ es un anillo. Por ejemplo, las tablas de sumar y multiplicar en $\mathbb{Z}_4$ son:

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

·	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Compárense con las de $\mathbb{Z}_5 = \{[0],[1],[2],[3],[4]\}$:

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

·	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

Las operaciones en $\mathbb{Z}_m$ están, pues, definidas a partir de las de $\mathbb{Z}$. Al intertar formalizar las relaciones entre ambos anillos, es útil considerar la aplicación de $\mathbb{Z}$

en $\mathbb{Z}_m$ llamada *proyección canónica*

$$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}_m.$$

Se deja como ejercicio comprobar que es un homomorfismo de anillos sobreyectivo.

Pero volvamos al caso $m = 4$. En la tabla de multiplicar de $\mathbb{Z}_4$ aparece un fenómeno insólito en nuestra aritmética común que además no aparece en $\mathbb{Z}_5$; hay un producto que se anula sin que sus factores sean nulos:

$$[2] \cdot [2] = [0].$$

Los anillos en los que esto **no** ocurre se denominan *dominios de integridad*, como sucede en $\mathbb{Z}$ ó en $\mathbb{Z}_5$; y a tales elementos de un anillo como $\mathbb{Z}_4$, esto es, aquellos que sin ser cero anulan a otros elementos distintos de cero con el producto, se les llama *divisores de cero*:

Definición. (1) Sea $R \neq \{0\}$ un anillo conmutativo. Un elemento $a \in R$ se llama *divisor de cero* (en R) si existe $b \neq 0$ en R tal que $ab = 0$. Un anillo R se denomina dominio de integridad si solamente tiene al 0 como divisor de cero.
(2) Sea $R \neq \{0\}$ un anillo. Un elemento $a \in R$ se dice que es una *unidad* en R si posee inverso multiplicativo.

Con la definición de unidad, se puede expresar el concepto de cuerpo de forma concisa: Un anillo conmutativo $R \neq \{0\}$ se dice que es un cuerpo si todo elemento de R distinto de cero es una unidad.

El anillo $\mathbb{Z}$ no posee divisores de cero distintos de cero, es decir, es un dominio de integridad, y sus únicas unidades son -1 y 1. Para anillos del tipo $\mathbb{Z}_m$ nuestro objetivo es mostrar cuándo no poseen divisores de cero.

Teorema 13.2. *Un anillo conmutativo R es un dominio de integridad si y solamente si se verifica la ley de cancelación:*

$$ab = ac, a \neq 0 \implies b = c.$$

Demostración. Demostremos primero la implicación "Dominio $\Longrightarrow$ Ley de cancelación", que es equivalente a "No se cumple ley de cancelación $\Longrightarrow$ No es dominio". Sean para ello $a, b, c \in R$ con $a \neq 0$ tal que $ab = ac \implies b \neq c$, esto es, $b - c \neq 0$. Como $a \neq 0$ y $b - c \neq 0$, entonces de las igualdades $a(b-c) = ab - ac = 0$ se deduce que existen divisores de cero no nulos, es decir, R no es un dominio. Recíprocamente, demostremos que si R no es un dominio, entonces no se cumple la ley de cancelación. Supongamos, pues, que existe $a \in R$, $a \neq 0$, tal que $ab = 0$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

para $b \neq 0$. Si se verificara la ley de cancelación, como $ab = a \cdot 0 (= 0)$ y $a \neq 0$, entonces se deduciría $b = 0$, lo que contradice tal ley. □

Teorema 13.3. *Todo dominio de integridad finito R es un cuerpo.*

Demostración. Veamos que todo $a \in R$, $a \neq 0$, es una unidad. Sea entonces $a \in R$, $a \neq 0$, y consideremos la aplicación "multiplicación por a", es decir

$$\begin{array}{rccc} \mu_a : & R & \to & R \\ & b & \mapsto & ab. \end{array}$$

La aplicación μ_a es inyectiva por el Teorema 13.2. Como R es finito, entonces μ_a también es sobreyectiva, y con ello una biyección; por tanto, existe $b \in R$ tal que $1 = \mu_a(b) = ab$. □

Teorema 13.4. *Sea $m \geq 2$. Las siguientes propiedades son equivalentes:*

(a) *$\mathbb{Z}_m$ es un dominio de integridad;*
(b) *$\mathbb{Z}_m$ es un cuerpo;*
(c) *m es un número primo.*

Demostración. (a) $\Longleftrightarrow$ (b): Es una consecuencia del Teorema 13.3, al ser $\mathbb{Z}_m$ finito.
(a) $\Longrightarrow$ (c): Probaremos su contrarrecíproco, es decir, $\neg$ (c) $\Longrightarrow$ $\neg$ (a). Sea m un número compuesto (es decir, no primo). Entonces existen $a, b \in \mathbb{Z}$ con $1 < a, b < m$ y $m = ab$. Consideremos $\pi : \mathbb{Z} \to \mathbb{Z}_m$ la proyección canónica; como $a, b < m$, es claro que

$$\pi(a) \neq [0] \quad \text{y} \quad \pi(b) \neq [0],$$

pero, al ser π un homomorfismo,

$$\pi(a)\pi(b) = \pi(ab) = \pi(m) = [0].$$

Luego $\mathbb{Z}_m$ posee divisores de cero aparte del [0] y por tanto, no puede ser un dominio de integridad.
(c) $\Longrightarrow$ (a): Sea m un número primo. Tomando de nuevo la proyección $\pi : \mathbb{Z} \to \mathbb{Z}_m$, si tuviéramos $a, b \in \mathbb{Z}$ tal que $\pi(a)\pi(b) = [0]$, entonces $\pi(ab) = [0]$, y así $ab = km$ para algún $k \in \mathbb{Z}$. Pero si esto es así, como m es primo, por el Teorema 12.7 (ver nota siguiente) o bien $m \mid a$, en cuyo caso $\pi(a) = [0]$, o bien $m \mid b$, y entonces $\pi(b) = [0]$; en cualquiera de los casos $\mathbb{Z}_m$ es un dominio de integridad. □

Nota: En la demostración anterior hemos usado el siguiente resultado: Sean $n, m \in \mathbb{Z}$, y sea p un número primo, entonces $p \mid mn \implies p \mid m \vee p \mid n$. La demostración se basa en el Lema de Bézout (Teorema 12.7): Supongamos que $p \nmid n$, entonces

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

hemos de probar que $p \mid m$. Para ello, como $\mathrm{mcd}(p,n) = 1$ al ser p primo, por la mencionada identidad existen $\alpha, \beta \in \mathbb{Z}$ tales que

$$1 = \alpha p + \beta n \Longleftrightarrow m \stackrel{(*)}{=} \alpha pm + \beta nm.$$

Por hipótesis, $p \mid mn$, es decir, existe $k \in \mathbb{Z}$ tal que $mn = kp$. Substituyendo en la igualdad $(*)$ se obtiene que

$$m = \alpha pm + \beta kp = (\alpha m + \beta k)p,$$

esto es, m es un múltiplo de p (pues claramente $\alpha m + \beta k \in \mathbb{Z}$), o lo que es lo mismo, $p \mid m$.

El Teorema 13.4 nos dice que, por ejemplo, el anillo cociente $\mathbb{Z}_5$ no tiene divisores de cero, porque es un cuerpo (y es un cuerpo porque 5 es un número primo), pero sí los tiene, como hemos comprobado, $\mathbb{Z}_4$, porque 4 no es primo. También podemos calcular las unidades de un anillo $\mathbb{Z}_m$. Si m es primo, todos sus elementos no nulos son unidades, al ser un cuerpo. Si m no es primo, es menos inmediato. En general se verifica:

Teorema 13.5. *Sean $a, m \in \mathbb{Z}$ con $m > 1$. La clase $[a]$ es una unidad en $\mathbb{Z}_m$ si y solamente si* $\mathrm{mcd}(a,m) = 1$.

Demostración. Si $\mathrm{mcd}(a,m) = 1$, entonces existen $\alpha, \beta \in \mathbb{Z}$ tales que $\alpha a + \beta m = 1$, y con ello es claro que $[\alpha][a] = [1]$, es decir, $[a]$ es invertible (unidad). Recíprocamente, si $[\alpha][a] = [1]$, entonces $[1] - [\alpha][a] = [1 - \alpha a] = [0] = [m]$, es decir, $1 - \alpha a = km$ para algún $k \in \mathbb{Z}$, y así $1 = \alpha a + km$, luego $\mathrm{mcd}(a,m) = 1$ por el Lema de Bézout 12.7. □

Un procedimiento análogo al que permite calcular inversos multiplicativos en el anillo $\mathbb{Z}_m$ nos muestra cómo resolver ecuaciones con una incógnita en los anillos cociente $\mathbb{Z}_m$. Consideremos $a, b, x \in \mathbb{Z}$ y la ecuación $[a][x] = [b]$ en $\mathbb{Z}_m$. Despejar la incógnita $[x]$ es en realidad resolver la siguiente congruencia:

$$ax \equiv b \mod m.$$

Para despejar x basta aplicar la definición de la relación de congruencia:

$$ax \equiv b \mod m \iff \exists\, y \in \mathbb{Z} \text{ tal que } ax - b = my.$$

Es decir, se trata de resolver la ecuación diofántica lineal en dos variables

$$ax - my = b.$$

Por la teoría aprendida en el capítulo 12, sabemos que tiene solución si y solamente si $\mathrm{mcd}(a,m)$ divide a b.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Ejemplo. Resolver la congruencia $17x \equiv 2 \mod 66$ pasa por resolver la ecuación diofántica $17x - 66y = 2$. Sabemos que tiene solución, pues $\text{mcd}(17,66) = 1$, que divide a 2. La identidad de Bézout se lee en este caso

$$1 = -31 \cdot 17 + 8 \cdot 66.$$

Por tanto, una solución de la ecuación diofántica es $x = -62, y = 16$, y el conjunto de todas sus soluciones es

$$\{(x,y) : x = -62 + \lambda \cdot 66, y = 16 - \lambda \cdot 17 \text{ para todo } \lambda \in \mathbb{Z}\}.$$

La solución a la congruencia de partida es

$$x = -62 + \lambda \cdot 66, \quad \text{para cualquier } \lambda \in \mathbb{Z}.$$

La solución simultánea de congruencias nos la ofrece un resultado que según la tradición procede de China:

Teorema 13.6 (Teorema chino de los restos)**.** *Sean $m,n \in \mathbb{Z}$ primos entre sí. Dados $a,b \in \mathbb{Z}$ arbitrarios, existe un $x \in \mathbb{Z}$ tal que*

$$x \equiv a \mod m \quad y \quad x \equiv b \mod n.$$

Además, $x' \in \mathbb{Z}$ es otra solución de ambas congruencias si y solamente si $x \equiv x'$ $\mod mn$.

El teorema se puede generalizar a un número arbitrario de congruencias. Veamos un ejemplo de resolución de un sistema de tres congruencias cuya abstracción constituiría una demostración del teorema chino:

Ejemplo. Se busca un entero x que satisfaga simultáneamente las congruencias

$$x \equiv 2 \mod 3, \quad x \equiv 3 \mod 4, \quad x \equiv 2 \mod 5.$$

Para ello, sea $M = \text{mcm}(3,4,5) = 3 \cdot 4 \cdot 5 = 60$, y hagamos $M_1 = M/3 = 20$, $M_2 = M/4 = 15$ y $M_3 = M/5 = 12$. Calculemos la identidad de Bézout para las parejas $(3,M_1)$, $(4,M_2)$ y $(5,M_3)$:

$$7 \cdot 3 + (-1) \cdot 20 = 1 \Longrightarrow e_1 := (-1) \cdot 20 = -20,$$
$$4 \cdot 4 + (-1) \cdot 15 = 1 \Longrightarrow e_2 := (-1) \cdot 15 = -15,$$
$$5 \cdot 5 + (-2) \cdot 12 = 1 \Longrightarrow e_3 := (-2) \cdot 12 = -24.$$

Una solución del sistema de congruencias propuesto es

$$x = 2 \cdot e_1 + 3 \cdot e_2 + 2 \cdot e_3 = -133.$$

como $-133 \equiv 47 \mod 60$, todas las demás soluciones son congruentes con 47 módulo 60.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

[Art] Artin, M.: Algebra. Birkhäuser, Basel 1993

[BRV] Basart, J. M., Rifà, J., Villanueva, M.: Fonaments de matemàtica discreta. Elements de combinatòria i d'aritmètica. Universitat Autònoma de Barcelona, 1999

[Big] Biggs, N.L.: Discrete Mathematics. Second ed. Oxford U.P., 2004

[GOV] Galindo Pastor, C., Orús Báguena, M.P., Vindel Cañas, M.P.: Problemes de matemàtica discreta. Universitat Jaume I, 1997

[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3 ed. McGraw Hill, 2007

[Rios] Ríos, S.: Matemática finita. Paraninfo, 1974

[SchWie] Schafmeister, O., Wiebe, H.: Grundzüge der Algebra. B.G. Teubner, 1978

[Wall2] Wallis, W.D.: A beginner's guide to discrete mathematics. Second edition. Birkhäuser, 2012

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Capítulo 14. Inclusión-Exclusión

Iniciamos aquí la última parte del curso, dedicada a la "combinatoria enumerativa", que bien podría llamarse "saber contar".[1] Contar está presente en nuestra vida cotidiana, pero ¿qué es contar?

Desde un punto de vista matemático, se puede decir que contar es establecer una biyección entre el conjunto de los elementos que queremos enumerar y un subconjunto de $\mathbb{N}$, como ya tratamos al final del capítulo 6. Esta sencilla reflexión nos ofrece un primer principio fundamental de conteo:

Teorema 14.1. *Sean A y B dos conjuntos. Si existe una biyección entre A y B, entonces $|A| = |B|$.*

Tan fácil como esta observación es la siguiente (a veces llamada "Principio de Dirichlet"):[2]

Teorema 14.2 (Principio del palomar)**.** *Si se tiene un palomar con n columbarios y $n+1$ palomas quieren ocupar uno de ellos, un columbario habrá de estar ocupado por más de una paloma.*

Este sencillo principio permite asegurar, por ejemplo, que en un grupo de 13 personas hay al menos dos que han nacido el mismo mes.

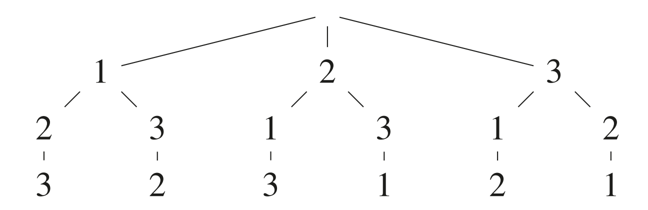
Cuando se tiene un problema de conteo para el que es posible enumerar todos los casos, una ayuda son los diagramas en árbol. Por ejemplo, supongamos que queremos establecer todas las biyecciones del conjunto $\{1,2,3\}$ en sí mismo (es decir, las "permutaciones" que se pueden efectuar con los elementos del conjunto $\{1,2,3\}$). En efecto, nos podemos servir de un diagrama en árbol:

[1] Saber contar no es fácil; recuérdese el viejo dicho: Hay tres clases de matemáticos, los que saben contar y los que no.

[2] Por el matemático alemán Johann Peter Gustav Lejeune DIRICHLET (1805–1859).

ISBN: 978-84-17900-65-6

DOI: http://dx.doi.org/10.6035/Sapientia170



Son 6 en total: 123, 132, 213, 231, 312, 321 (leyendo de arriba a abajo). Veremos en el capítulo 15 que este 6 se esconde bajo el traje de $3! = 3 \cdot 2 \cdot 1$.

Existen otras dos reglas básicas de conteo:

(i) Si un suceso S puede ocurrir de m formas y otro suceso T puede ocurrir de n formas, sin que sea simultáneo a S, entonces o bien S o bien T puede ocurrir de $m+n$ formas. Si S y T son vistos como conjuntos disjuntos, entonces este principio se expresa como

$$|S \cup T| = |S| + |T|.$$

Si los conjuntos no fueran disjuntos la fórmula ha de modificarse, como veremos después.

(ii) Si un suceso S ocurre de m formas e, independiente a él, otro suceso T ocurre de n formas, ambos ocurren de mn formas. Vistos S y T como conjuntos, este principio se traduce así:

$$|S \times T| = |S| \cdot |T|.$$

Ejemplo. En la UJI se imparten dos cursos diferentes de matemáticas, tres cursos diferentes de informática y cinco cursos diferentes de economía. El número de formas en que un alumno puede elegir un curso de cada área (matemáticas, informática, economía) es $2 \cdot 3 \cdot 5 = 30$, de acuerdo con (ii). El número de formas en que un alumno puede elegir solamente uno de los cursos ofertados es, según (i), igual a $2+3+5 = 10$.

Decíamos que la fórmula en (i) para el cardinal de la unión de dos conjuntos precisa de una corrección si estos no son disjuntos: efectivamente, no es difícil ver que si $A \cap B \neq \varnothing$, entonces

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Si tuviéramos tres conjuntos A_1, A_2, A_3 no disjuntos, la estructura de álgebra de Boole subyacente nos permite calcular, junto a la igualdad anterior:

$$\begin{aligned}|A_1 \cup A_2 \cup A_3| =& |A_1 \cup (A_2 \cup A_3)| = |A_1| + |A_2 \cup A_3| - |A_1 \cap (A_2 \cup A_3)| \\ &\vdots \\ =& |A_1| + |A_2| + |A_3| - (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) + |A_1 \cap A_2 \cap A_3|.\end{aligned}$$

Para poder escribir una regla general válida para n conjuntos, necesitamos la notación siguiente: Para $T \subseteq \{1, \ldots, n\}$, con $T \neq \varnothing$, es

$$A_T := \bigcap_{i \in T} A_i.$$

El análisis de las fórmulas para dos y tres conjuntos motiva la idea de que, en las sumas de la fórmula, los cardinales de los subconjuntos $T \subseteq \{1, \ldots, n\}$ con $|T|$ impar están provistos de signo positivo, en tanto que los otros llevan signo negativo. En efecto, la fórmula general es:

Teorema 14.3 (Principio de Inclusión-Exclusión)**.** *Si $A_1, A_2, \ldots, A_n$ conjuntos finitos, entonces*

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{\substack{T \subseteq \{1, \ldots, n\} \\ T \neq \varnothing}} (-1)^{|T|+1} |A_T|.$$

Dejamos la demostración a un lado para ilustrar el principio con dos ejemplos muy representativos.

El primero responde a una pregunta sencilla: ¿cuántos de los números naturales $1, 2, \ldots, 100$ son divisibles por 2, por 3 o por 5? El principio de inclusión-exclusión ayuda. Denotemos por V_i al conjunto de los números entre 1 y 100 que son divisibles por i, entonces:

$$\begin{aligned}|V_2 \cup V_3 \cup V_5| =& |V_2| + |V_3| + |V_5| - (|V_2 \cap V_3| + |V_2 \cap V_5| + |V_3 \cap V_5|) + |V_2 \cap V_3 \cap V_5| \\ =& |V_2| + |V_3| + |V_5| - (|V_6| + |V_{10}| + |V_{15}|) + |V_{30}| \\ =& 50 + 33 + 20 - (16 + 10 + 6) + 3 = \mathbf{74}.\end{aligned}$$

Un ejemplo más complicado trata del conteo de las biyecciones de un conjunto $\{1, \ldots, n\}$ en sí mismo que no tenga puntos fijos (es decir, las permutaciones de n elementos sin puntos fijos). Veamos.

Dada una permutación $a_1 a_2 \cdots a_n$ de $\{1, 2, \ldots, n\}$, entonces $i \in \{1, 2, \ldots, n\}$ se llama *punto fijo* si $a_i = i$, es decir, si el elemento i permanece en su puesto tras

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

efectuar la permutación. Denotemos

$$A_i := \{\text{permutación de } \{1,2,\ldots,n\} \text{ con punto fijo } i\}.$$

Ya hemos mencionado (y lo veremos en el capítulo 15) que el conjunto de las permutaciones de $\{1,2,\ldots,n\}$ posee cardinal $n!$. Por tanto, las que no dejan ningún punto fijo son tantas como

$$n! - |A_1 \cup A_2 \cup \cdots \cup A_n|.$$

Si $T \subseteq \{1,2,\ldots,n\}$, entonces es

$$A_T = \{\text{permutación de } \{1,2,\ldots,n\} \text{ con puntos fijos } i \in T\}$$

(pero posiblemente con más puntos fijos que ésos). En el conjunto A_T están todas las permutaciones en las que se permuta (valga la redundancia) el conjunto $\{1,\ldots,n\} \setminus T$. Entonces

$$|A_T| = (n - |T|)!$$

Así, el Principio de inclusión-exclusión 14.3 asegura que

$$\begin{aligned} n! - |A_1 \cup \cdots \cup A_n| =& n! - \sum_{i=1}^{n} (-1)^{i+1} \binom{n}{i} (n-1)! \\ =& n! - \sum_{i=1}^{n} (-1)^i (-1) \frac{n!}{(n-i)!i!} (n-i)! \\ =& n! + \sum_{i=1}^{n} (-1)^i \frac{n!}{i!} \\ & n! \Big(1 + \sum_{i=1}^{n} (-1)^i \frac{1}{i!}\Big) \\ =& n! \cdot \sum_{i=0}^{n} \frac{(-1)^i}{i!}. \end{aligned}$$

Démonos cuenta de que

$$\lim_{n\to\infty} \sum_{i=0}^{n} \frac{(-1)^i}{i!} = \frac{1}{e} = \frac{1}{2.718\ldots} \cong 0.368;$$

es decir, incluso ya para números n moderadamente grandes, la proporción de permutaciones sin punto fijo es de aproximadamente 0.368 de todas las permutaciones.

Un problema concreto en el que aparecen permutaciones sin puntos fijos es el siguiente: en un guardarropa, por ejemplo en el teatro, se devuelven los abrigos entregados al principio de la función sin orden ni concierto; entonces, la probabilidad de que nadie reciba su propio abrigo es de 0.368.

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

Concluimos el capítulo con el llamado *principio del doble conteo*. Trivialmente se tiene que, si contamos (bien) los elementos de un conjunto finito de dos maneras y se obtienen α y β como resultados de cada conteo, entonces $\alpha = \beta$. Presentamos ahora una estrategia de conteo basada en este intuitivo principio. Para ello consideremos en primer lugar una definición: Un *sistema de incidencia* es una terna (A,B,R) formada por dos conjuntos A y B y una correspondencia de A en B. Se dice que dos elementos $a \in A$ y $b \in B$ son "incidentes" si aRb; en otro caso a y b se llaman "no incidentes".

Un ejemplo clásico, de donde se toma el nombre, es considerar puntos, rectas y la relación de incidencia R definida así: un punto p está relacionado con una recta r mediante la correspondencia R, es decir, pRr, si y solamente si p pertenece a la recta r.

Se dice que un sistema de incidencia (A,B,R) es finito si A y B son conjuntos finitos. En ese caso, dados $a \in A$ y $b \in B$, se definen los cardinales

$$d(a) = |\{b \in B : a,b \text{ son incidentes}\}|$$
$$d(b) = |\{a \in A : a,b \text{ son incidentes}\}|.$$

Teorema 14.4 (Principio del doble conteo)**.** *Sea (A,B,R) un sistema de incidencia finito, entonces*

$$\sum_{a\in A} d(a) = \sum_{b\in B} d(b).$$

Demostración. Sean $A = \{a_1,\dots,a_k\}$ y $B = \{b_1,\dots,b_\ell\}$, y consideramos la matriz $M = (m_{ij})$ con

$$m_{ij} = \begin{cases} 1 & \text{si } a_i\, R\, b_j \\ 0 & \text{si no.} \end{cases}$$

(Esta matriz se llama la *matriz de incidencia* del sistema).

El número $d(a_i)$ es justo el número de 1's que aparecen en la fila i-ésima de M, de donde se deduce que

$$\sum_{a\in A} d(a) = \sum_{i=1}^{k} d(a_i) = \sum_{i=1}^{k}\sum_{j=1}^{\ell} m_{ij}.$$

Por otro lado, $d(b_j)$ es el número de 1's en la j-ésima columna de M, de donde se sigue que

$$\sum_{b\in B} d(b) = \sum_{j=1}^{\ell} d(b_j) = \sum_{j=1}^{\ell}\sum_{i=1}^{k} m_{ij}.$$

En total se obtiene

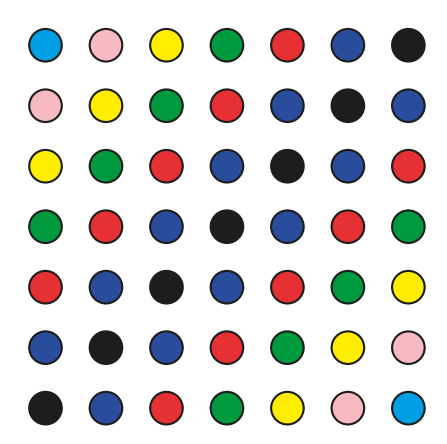
$$\sum_{a\in A} d(a) = \sum_{i=1}^{k}\sum_{j=1}^{\ell} m_{ij} = \sum_{j=1}^{\ell}\sum_{i=1}^{k} m_{ij} = \sum_{b\in B} d(b).$$

□

Ejemplo. El Teorema 14.4 permite dar otra prueba de la fórmula

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

alternativa a la vista en el capítulo 2 como aplicación del principio de inducción. Consideremos un cuadrado de puntos de tamaño $(n+1)\times(n+1)$. El diagrama contiene obviamente $(n+1)^2$ puntos. Pero otra de forma de contar los puntos del diagrama es por diagonales ("rebanadas" del cuadrado). La diagonal (de puntos negros en la figura inferior) tiene $n+1$ puntos, y según nos vamos distanciando de ella por arriba o por abajo, las "paralelas" a la diagonal cuentan $\sum_{i=1}^{k} i$ puntos cada una, para $k = n,\ldots,1$.



Sumando todas las rebanadas, incluyendo la diagonal, queda

$$(n+1) + 2\cdot\sum_{i=1}^{n} i = (n+1)^2,$$

de donde se obtiene la fórmula deseada:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Ejemplo. Supongamos que "ser amigo de" es una relación simétrica. En una clase se sientan 64 alumnos (con "o"), y n alumnas (con "a"). Cada alumno es amigo de exactamente 5 alumnas y cada alumna es amiga de exactamente 8 alumnos. ¿Cuántas alumnas hay en esa clase?

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Denotemos a los alumnos por "o" y a las alumnas por "a". En la notación del Teorema 14.4, A es el conjunto de alumnos y B el de alumnas (o al revés, tanto da). El conjunto de las relaciones de amistad es

$$R = \{(o,a) : o \in A, a \in B, o \text{ y } a \text{ son amigos}\}.$$

Como en el teorema, definimos

$$d(a) = |\{(o,a) : a \in B\}|$$
$$d(b) = |\{(o,a) : o \in A\}|.$$

Por el Principio del doble conteo 14.4 se tiene que

$$5 \cdot 64 = \sum_{o \in A} d(o) = \sum_{a \in B} d(a) = 8n,$$

pues cada alumno conoce exactamente a 5 alumnas y cada alumna a 8 alumnos. Por lo tanto

$$5 \cdot 64 = 8n \Longleftrightarrow n = \frac{1}{8} \cdot 5 \cdot 2^6 = 5 \cdot 2^3 = 40.$$

La clase tiene, pues, 40 alumnas.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

[Aig] Aigner, M.: A course in enumeration. Springer, 2007
[BRV] Basart, J. M., Rifà, J., Villanueva, M.: Fonaments de matemàtica discreta. Elements de combinatòria i d'aritmètica. Universitat Autònoma de Barcelona, 1999
[Big] Biggs, N.L.: Discrete Mathematics. Second ed. Oxford U.P., 2004
[Conr] Conradie, W., Goranko, V.: Logic and Discrete Mathematics. A concise introduction. Wiley, 2015
[FEA] Franco, J.R., Espinel, M.C., Almeida, P.R.: Manual de combinatoria. Abecedario, 2008
[Gall] Gallier, J.: Discrete Mathematics. Springer, 2011
[HHM] Harris, J.M., Hirst, J.L., Mossinghoff, M.J.: Combinatorics and Graph Theory. Second edition. Springer, 2010
[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3. ed. McGraw Hill, 2007
[Mar] Martin, G.E.: Counting: the art of enumerative combinatorics. Springer, 2001.
[PTW] Pólya, G., Tarjan, R.E., Woods, D.R.: Notes on introductory combinatorics. Birkhäuser, 2010
[Rib] Ríbnikov, K.: Análisis combinatorio. Mir Moscú, 1988
[Trias] Trias Pairó, J.: Matemàtica discreta. Problemes resolts. Universitat Politècnica de Catalunya, 2009
[Wall2] Wallis, W.D.: A beginner's guide to discrete mathematics. Second edition. Birkhäuser, 2012

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Capítulo 15. Extracciones y selecciones

La noción de “experimento aleatorio” proviene del área del cálculo de probabilidades y estadística. En vez de experimento aleatorio podemos decir “extracción aleatoria” o “sorteo”, lo que inevitablemente nos lleva a pensar en los sorteos de la Lotería Primitiva, ONCE, Euromillón, de Lotería Nacional, etc.

En el sorteo de la primitiva se extraen aleatoriamente 6 bolas de una urna con 49, numeradas del 1 al 49. Una bola extraída no se devuelve a la urna, y para el anuncio de los resultados no juega ningún papel en qué orden se sacan las bolas: se trata de una extracción no ordenada (desde el punto de vista temporal).

Podemos clasificar extracciones de este tipo en cuatro categorías, a saber:

(1) Extracciones ordenadas con reposición de bolas.
(2) Extracciones ordenadas sin reposición.
(3) Extracciones no ordenadas con devolución.
(4) Extracciones no ordenadas sin reposición.

El sorteo de la bonoloto se encuadra en la categoría (4). Las extracciones con reposición aparecen en el juego de los dados, por ejemplo, si identificamos el lanzamiento de un dado con la extracción de una bola de una urna con seis bolas.

En este capítulo queremos determinar cuántos experimentos o extracciones de k bolas se pueden efectuar de una urna con n bolas para cada uno de los cuatro tipos anteriores. El caso más difícil es (3), que dejaremos para el final. El más sencillo es sin duda el caso (1).

Si se quieren realizar k extracciones de la urna con las n bolas, y las bolas extraídas las devolvemos a la urna tras cada extracción, podemos formar todas las k-tuplas

$$(s_1, \ldots, s_k), \quad s_i \in \{1, \ldots, n\}$$

y cada k-tupla se corresponde exactamente con una extracción. Es decir, se tiene:

Teorema 15.1. *Hay exactamente n^k extracciones ordenadas con devolución de k elementos en un conjunto con n elementos.*

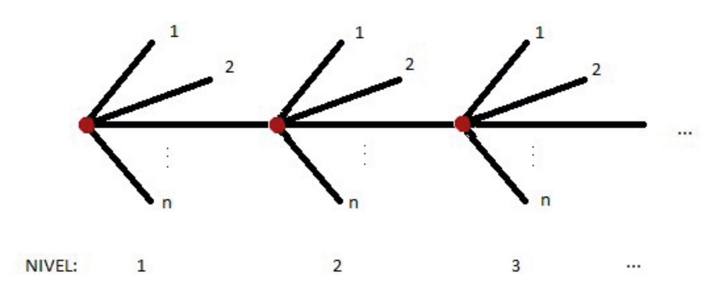
ISBN: 978-84-17900-65-6

DOI: http://dx.doi.org/10.6035/Sapientia170

Demostración. Se han de contar los elementos del producto cartesiano N^k, donde N es un conjunto con n elementos; este problema de conteo lo resuelve la regla básica de conteo (ii) del capítulo anterior. □

Nuestro conjunto estándar de n elementos es $\{1,\ldots,n\}$, y para el conteo en experimentos aleatorios como el anterior podemos suponer que $N = \{1,\ldots,n\}$.

De gran ayuda para el conteo de muestras aleatorias son los diagramas en árbol. La situación del Teorema 15.1 se describe mediante el diagrama



Se trata de un árbol con un nodo o vértice llamado *raíz*. De cada nodo salen n ramas y esto se repite k veces, es decir, a lo largo de k niveles. Cada extracción corresponde a un camino en el árbol, desde la raíz hasta un extremo, y por cada extremo pasa exactamente un camino, que diremos que tiene longitud k.

Ejemplo. Tres galgos pueden perseguir a dos liebres de $2^3 = 8$ maneras distintas; dos galgos pueden perseguir a tres liebres de $3^2 = 9$ maneras distintas.

Nota. Nótese que n^k es el número de aplicaciones de un conjunto de k elementos en un conjunto de n elementos.

En la prueba del Teorema 15.1 hemos supuesto que ya sabíamos que el número de elementos de N^k es n^k. Este hecho se puede demostrar por inducción con ayuda de un diagrama en árbol: Tras $k-1$ niveles el árbol tiene n^{k-1} extremos y cada uno de los caminos que pasan por ellos se puede prolongar al nivel k de n maneras exactamente. Por lo tanto, se deduce que hay $n \cdot n^{k-1} = n^k$ caminos de longitud k.

Los diagramas en árbol son también de gran utilidad para conteos de muestras aleatorias ordenadas *sin reposición*. Antes de dar una respuesta definitiva vamos a investigar una *fórmula recursiva*. Sea $S(n,k)$ el número buscado de extracciones posibles ordenadas de k bolas de un conjunto de n sin devolverlas a la urna una vez

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

sacadas, con $n \in \mathbb{N}$ y $0 \leq k \leq n$. Nuestro árbol tiene entonces $S(n,k-1)$ vértices en el nivel $k-1$. Por cada uno se han utilizado $k-1$ bolas, con lo que solamente quedan en la urna $n-(k-1) = n-k+1$ bolas. Es decir, se tiene

$$S(n,k) = S(n,k-1) \cdot (n-k+1).$$

Para precisar el concepto hemos de darnos cuenta de que una muestra aleatoria ordenada con k elementos sin reposición en el conjunto $N = \{1,\dots,n\}$ es una k-tupla

$$(s_1,\dots,s_k) \in N^k$$

donde los s_i son distintos dos a dos.

El objetivo es dar una fórmula cerrada para $S(n,k)$.

Si empezamos con $k = 0$, se ve que $S(n,0) = 1$, pues 0 bolas se pueden extraer exactamente de una forma. Sucesivamente se comprueba

$$\begin{aligned}
S(n,1) =& S(n,0) \cdot n = n \\
S(n,2) =& S(n,1) \cdot (n-1) = n(n-1) \\
S(n,3) =& S(n,2) \cdot (n-2) = n(n-1)(n-2) \\
&\vdots \\
S(n,k) =& S(n,k-1) \cdot (n-k+1) = n(n-1)\cdots(n-k+1)
\end{aligned}$$

Para el producto del lado derecho escribiremos

$$[n]_k := n(n-1)\cdots(n-k+1).$$

y lo denominaremos *factorial decreciente*, o *factorial generalizado*, o más frecuentemente *símbolo de Pochhammer*.[1]

Teorema 15.2. *De un conjunto de n elementos se pueden extraer exactamente $[n]_k$ muestras aleatorias ordenadas sin reposición.*

Demostración. Solamente tenemos que escribir formalmente la discusión anterior de acuerdo al principio de inducción. Para $k = 0$ es evidente que $S(n,0) = 1$, y dada la hipótesis de inducción para $k-1$, el paso inductivo es fácil:

$$\begin{aligned}
S(n,k) =& S(n,k-1) \cdot (n-k+1) \\
=& [n]_{k-1} \cdot (n-k+1) \\
=& [n]_k,
\end{aligned}$$

para cualquier $k > 0$. □

[1] Honrando la memoria del matemático alemán Leo August POCHHAMMER (1841–1920).

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

Ejemplo. ¿Cuántos números de tres cifras distintas se pueden formar con los números $3,4,5,6$ y 7? Pues exactamente $[5]_3 = 5 \cdot 4 \cdot 3 = 60$.

Nota: El Teorema 15.2 cuenta el número de aplicaciones inyectivas de un conjunto con k elementos en un conjunto con n elementos, para $k \leq n$.

El caso particular $k = n$ es especialmente importante. Se trata de

$$[n]_n = n!,$$

el *factorial* de n, que ya definimos (de otra manera) en el capítulo 2. Los valores de $n!$ para valores pequeños de n se deberían conocer:

$$\begin{array}{ll} 0! = 1 & 4! = 24 \\ 1! = 1 & 5! = 120 \\ 2! = 2 & 6! = 720 \\ 3! = 6 & 7! = 5040 \end{array}$$

Las muestras aleatorias ordenadas de tamaño n sin reposición de un conjunto N de n elementos se denominan también *permutaciones* (u *ordenaciones*) de N. (Ya nos las hemos encontrado anteriormente, por ejemplo en el capítulo 14 o en el 11). Cada una de las muestras representa exactamente una posibilidad de ordenar los n elementos de N de una forma determinada.

Obsérvese que $n!$ es el número de aplicaciones biyectivas que se pueden establecer entre un conjunto de n elementos y otro conjunto de n elementos.

Contar muestras aleatorias no ordenadas es considerablemente más complicado. Para ello hemos de aprender dos nuevos principios de conteo. Consideremos en primer lugar muestras aleatorias no ordenadas sin reposición, un “sorteo de lotería generalizado” en el sentido siguiente.

En un sorteo de lotería primitiva normal se empieza extrayendo una muestra ordenada, y después se identifican las muestras que difieren solamente en el orden. Para ello, se clasifican las muestras ordenadas: dos muestras pertenecen a la misma clase si y solamente si difieren en el orden. Cada muestra ordenada sin reposición tiene la forma

$$(s_1, \ldots, s_k)$$

donde los s_i forman elementos de $\{1, 2, \ldots, n\}$ distintos dos a dos. Nótese que, si se olvidara el orden, tendríamos simplemente un subconjunto de k elementos

$$\{s_1, \ldots, s_k\} \subseteq N$$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

y cada uno de estos representa exactamente una muestra no ordenada sin reposición, de acuerdo con lo expuesto anteriormente.

Ahora bien, acabamos de ver que los elementos de los conjuntos de k elementos $\{s_1,\ldots,s_k\}$ se pueden ordenar de $k!$ formas. Entonces se tiene que cada $k!$ muestras ordenadas dan lugar a la misma muestra no ordenada. Las muestras no ordenadas sin reposición se representan por sucesiones monótonas *estrictamente* crecientes $(s_1,\ldots,s_k) \in N^k$.

Los números

$$\binom{n}{k} = \frac{[n]_k}{k!} = \frac{n!}{k!(n-k)!}, \quad n,k \in \mathbb{N}$$

se llaman *coeficientes binomiales*, porque también aparecen en la fórmula del binomio de Newton, cf. Teorema 2.3.

Ya hemos justificado que las $[n]_k$ muestras ordenadas se pueden agrupar en paquetes con $k!$ muestras cada uno, que representan la misma muestra no ordenada. El número de paquetes será entonces $\binom{n}{k}$:

Teorema 15.3. *De un conjunto de n elementos se pueden extraer exactamente $\binom{n}{k}$ muestras no ordenadas sin reposición.*

El principio de conteo que hemos aplicado en la demostración del Teorema 15.3 se deja formular sencillamente

Teorema 15.4. *Sea M un conjunto finito y sean $N_1,\ldots,N_m$ subconjuntos de M disjuntos dos a dos. Entonces*

$$|M| = |N_1| + \ldots + |N_m|.$$

Si $|N_i| = |N_j| = n$ para todos i y j, entonces

$$m = \frac{|M|}{n}.$$

Casi no hay nada que probar: solamente se precisa recordar que $|X \cup Y| = |X| + |Y|$ si los conjuntos X e Y son disjuntos.

Ejemplo. El profesor de Matemáticas propone una lista de 15 ejercicios de los que los alumnos tienen que resolver 4. El alumno tendrá entonces

$$\binom{15}{4} = \frac{15!}{4!(15-4)!} = \frac{15!}{4!11!} = 1365$$

elecciones posibles.

El principio del Teorema 15.4, que tan útil resulta para contar reuniendo en paquetes muestras ordenadas sin reposición, tropieza con un grave inconveniente para contar muestras *con* reposición: ¡los paquetes pueden tener diferente número de elementos! Consideremos el caso $n = 6, k = 2$, el lanzamiento de dos dados. La muestra ordenada $(1,1)$ forma un paquete con exactamente un elemento; por el contrario, $(2,1)$ y $(1,2)$ forman un paquete con dos elementos.

Si generalizamos esta observación para n arbitrario y $k = 2$, nos daremos cuenta de que hay n muestras de tipo (x,x) y $\binom{n}{2}$ de tipo (x,y) con $x \neq y$. Para $k = 2$ obtenemos

$$n + \binom{n}{2} = n + \frac{n(n-1)}{2} = \frac{n(n-1)+2n}{2} = \frac{n(n+1)}{2} = \binom{n+1}{2}$$

muestras no ordenadas sin reposición de un conjunto de n elementos. Ya para $k = 3$ el análisis de las distintas situaciones que se plantean es más delicado, y es evidente que el caso general no se va a poder resolver de este modo.

Anteriormente interpretamos las muestras no ordenadas sin reposición como sucesiones monótonas estrictamente crecientes

$$(s_1,\ldots,s_k), \quad 1 \leq s_1 < \cdots < s_k \leq n.$$

De la misma manera, las muestras no ordenadas con repetición se corresponden con sucesiones monótonas crecientes

$$(s_1,\ldots,s_k) \in N^k$$

con $1 \leq s_1 \leq \cdots \leq s_k \leq n$. Dada una tal sucesión, consideremos la sucesión

$$\varphi(s_1,\ldots,s_k) = (s_1, s_2+1, \ldots, s_k+k-1).$$

Esta nueva sucesión es monótona *estrictamente* creciente y toma sus valores entre 1 y $n+k-1$. Se puede demostrar que φ es una biyección:

Teorema 15.5. *Sea X el conjunto de las sucesiones monótonas crecientes $s_1,\ldots,s_k$ con*

$$1 \leq s_1 \leq \cdots \leq s_k \leq n$$

e Y el conjunto de las sucesiones monótonas estrictamente crecientes $t_1,\ldots,t_k$ con

$$1 \leq t_1 < \cdots < t_k \leq n+k-1.$$

Entonces $\varphi : X \to Y$ es una aplicación biyectiva.

Demostración. Basta advertir que la aplicación $\psi : Y \to X$ dada por

$$\psi(t_1,\ldots,t_k) = (t_1, t_2-1, \ldots, t_k-(k-1))$$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

es la inversa de la aplicación φ, pues $\varphi \circ \psi = \mathrm{id}_Y$ y que $\psi \circ \varphi = \mathrm{id}_X$. □

Como consecuencia se verifica:

Teorema 15.6. *De un conjunto con n elementos se pueden extraer exactamente* $\binom{n+k-1}{k}$ *muestras no ordenadas de tamaño k con reposición.*

Hemos reducido un problema de conteo difícil a un problema previamente resuelto mediante una transformación elegante.

Ejemplo. En una cafetería se sirven 6 tipos diferentes de café. ¿De cuántas maneras se pueden elegir tres cafés? Como no importa en qué orden elijamos los cafés, y no está prohibido elegir cafés del mismo tipo, se tendrán

$$\binom{6+3-1}{3} = \binom{8}{3} = \frac{8!}{3!5!} = 56$$

elecciones posibles.

Resumimos las reflexiones anteriores en el cuadro siguiente:

	MUESTRAS ALEATORIAS		
	Reposición	Interpretación con sucesiones	Cantidad
Ordenadas	Sí	$(s_1,\ldots,s_k)$ en $\mathbb{N}^k$	n^k
Ordenadas	No	$(s_1,\ldots,s_k)$ en $\mathbb{N}^k$ $s_i \neq s_j$ para $i \neq j$	$[n]_k$
No ordenadas	Sí	$(s_1,\ldots,s_k)$ en $\mathbb{N}^k$ $1 \leq s_1 \leq s_2 \leq \cdots \leq s_k \leq n$	$\binom{n+k-1}{k}$
No ordenadas	No	$(s_1,\ldots,s_k)$ en $\mathbb{N}^k$ $1 \leq s_1 < s_2 < \cdots < s_k \leq n$	$\binom{n}{k}$

Terminamos generalizando la idea de la clasificación que nos ha llevado a los coeficientes binomiales. Consideremos muestras ordenadas de longitud n, en las que s_1 aparece k_1 veces, s_2 aparece k_2 veces, ... , s_m aparece k_m veces. Por supuesto $k_1 + k_2 + \cdots + k_m = n$. Para su visualización podemos imaginarnos un cajón de

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

imprenta en el que la letra s_1 está k_1 veces, la letra s_2 está k_2 veces... y la letra s_m está k_m veces, y se quiere determinar cuántas palabras de longitud

$$n = k_1 + k_2 + \cdots + k_m$$

se pueden formar con esas letras.

La idea es hacer distinguibles los ejemplares de cada letra, de forma que se tengan n símbolos distinguibles y posteriormente identificar aquellas palabras que se diferencien solamente por permutaciones de los ejemplares de las letras individuales. Con ellos está clara la solución: Los k_1 ejemplares de la letra s_1 se pueden permutar $k_1!$ veces, etc. Por tanto:

Teorema 15.7. *El número de muestras ordenadas en las que aparece s_i exactamente k_i veces, con $i = 1, \ldots, m$, es*

$$\frac{n!}{k_1! \cdots k_m!}, \quad n = k_1 + \cdots + k_m.$$

Este número se llama *coeficiente multinomial* y se denota por

$$\binom{n}{k_1 \cdots k_m}.$$

Demostración. De n símbolos se tienen $n!$ muestras ordenadas de tamaño n sin reposición, y de ellas se agrupan cada vez $k_1!, k_2!, \ldots, k_m!$ en una misma clase. □

Ejemplo. ¿Cuántas palabras (aunque no estén en el DRAE[2]) de 11 letras se pueden formar con las letras de la palabra MISSISSIPPI permutándolas entre sí? Veamos: la palabra MISSISSIPPI tiene 11 letras, de las que l P se repite dos veces, la I se repite 4 veces y la S otras tantas. Así tendremos

$$\binom{11}{1\ 2\ 4\ 4} = \frac{11!}{1!\ 2!\ \ 4!\ 4!} = 34650$$

palabras.

Los coeficientes multinomiales deben su exótico nombre a la siguiente generalización del Teorema del binomio de Newton 2.3:

Teorema 15.8. *Para todos $n, m \in \mathbb{N}$ con $m \geq 2$ y para todas las indeterminadas $a_1, \ldots, a_m$ que conmuten dos a dos se verifica que*

$$(a_1 + \cdots + a_m)^n = \sum_{\substack{k_1,\ldots,k_m \geq 0 \\ k_1+\cdots+k_m = n}} \binom{n}{k_1 \cdots k_m} a_1^{k_1} \cdots a_m^{k_m}.$$

[2]Diccionario de la Real Academia de la Lengua Española.

Terminamos el capítulo con una sencilla observación sobre coeficientes multinomiales. Si $n = k_1 + k_2$, se tiene que

$$\binom{n}{k_1} = \binom{n}{k_1\ k_2} = \binom{n}{k_2}.$$

La primera igualdad se puede demostrar mediante un sencillo cálculo:

$$\begin{aligned}
\binom{n}{k_1} &= \frac{n(n-1)\cdots(n-k_1+1)}{k_1!} \\
&= \frac{n(n-1)\cdots(n-k_1+1)k_2(k_2-1)\cdots 2\cdot 1}{k_1!k_2!} \\
&= \frac{n!}{k_1!k_2!} \\
&\overset{(*)}{=} \binom{n}{k_1\ k_2},
\end{aligned}$$

donde $(*)$ se deduce de $n = k_1 + k_2$. A la vista de

$$\binom{n}{k_1\ k_2} = \binom{n}{k_2\ k_1},$$

la segunda igualdad también está clara.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

[Aig] Aigner, M.: A course in enumeration. Springer, 2007

[BRV] Basart, J. M., Rifà, J., Villanueva, M.: Fonaments de matemàtica discreta. Elements de combinatòria i d'aritmètica. Universitat Autònoma de Barcelona, 1999

[Big] Biggs, N.L.: Discrete Mathematics. Second ed. Oxford U.P., 2004

[Conr] Conradie, W., Goranko, V.: Logic and Discrete Mathematics. A concise introduction. Wiley, 2015

[FG] Ferrando, J.C., Gregori, V.: Matemática Discreta. 2. ed. Reverté, 2002

[FEA] Franco, J.R., Espinel, M.C., Almeida, P.R.: Manual de combinatoria. Abecedario, 2008

[Gall] Gallier, J.: Discrete Mathematics. Springer, 2011

[HHM] Harris, J.M., Hirst, J.L., Mossinghoff, M.J.: Combinatorics and Graph Theory. Second edition. Springer, 2010

[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3. ed. McGraw Hill, 2007

[Mar] Martin, G.E.: Counting: the art of enumerative combinatorics. Springer, 2001

[PTW] Pólya, G., Tarjan, R.E., Woods, D.R.: Notes on introductory combinatorics. Birkhäuser, 2010

[Rib] Ríbnikov, K.: Análisis combinatorio. Mir Moscú, 1988

[Trias] Trias Pairó, J.: Matemàtica discreta. Problemes resolts. Universitat Politècnica de Catalunya, 2009

[Wall2] Wallis, W.D.: A beginner's guide to discrete mathematics. Second edition. Birkhäuser, 2012

Capítulo 16.
Funciones y generatrices

Las funciones generatrices son una herramienta general que se enmarca dentro de las series de números reales, pero sin considerar cuestiones de convergencia, propias del análisis matemático. Su uso generalizado en combinatoria, que es el que se introduce en este capítulo, fue propiciado por el matemático húngaro George PÓLYA (1887–1985), ver por ejemplo [**PTW**].

Sea $(a_k)_{k\geq 0} = (a_0, a_1, a_2, \ldots)$ una sucesión de números reales. Una *función generatriz* para la sucesión $(a_k)_{k\geq 0}$ es una serie de potencias

$$\sum_{k=0}^{\infty} a_k x^k,$$

donde la x ha de interpretarse como una indeterminada, pero no como una variable real. En este sentido se dice que la anterior es una serie de potencias *formales*.

Las series de potencias formales se pueden sumar "término a término", es decir, de acuerdo a la regla siguiente:

$$\left(\sum_{i=0}^{\infty} a_i x^i\right) + \left(\sum_{j=0}^{\infty} b_j x^j\right) := \left(\sum_{k=0}^{\infty} c_k x^k\right) \qquad \text{donde } \ c_k = a_k + b_k.$$

También se puede definir un producto de series de potencias formales, llamado *producto de Cauchy*, como sigue:

$$\left(\sum_{i=0}^{\infty} a_i x^i\right) \cdot \left(\sum_{j=0}^{\infty} b_j x^j\right) := \left(\sum_{k=0}^{\infty} c_k x^k\right) \quad \text{donde } \ c_k = \sum_{i+j=k} a_i + b_j.$$

Conociendo el término general de una sucesión es inmediato el cálculo término a término de su función generatriz. Por ejemplo, si la sucesión en cuestión posee término general $a_k = k+3$, para $k = 0, 1, 2, \ldots$, su función generatriz es la serie

$$F(x) = \sum_{k=0}^{\infty} (k+3)x^k.$$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Un asunto diferente es la convergencia de las series tratadas. Al considerarlas avatares puramente *formales*, se excluye de su análisis en este contexto cualquier consideración relativa al radio de convergencia de las series, una problemática propia del análisis matemático

Ejemplos. (a) La función generatriz de la sucesión constante $1,1,1,1,\dots$ es

$$F(x) = 1+x+x^2+x^3+x^4+\cdots = \frac{1}{1-x}.$$

(b) Un caso particular de sucesión es aquella tal que todos sus términos son cero de un lugar en adelante; es decir, es una sucesión con un número finito de términos, si así se quiere ver. Por ejemplo, la sucesión

$$1,1,1,1,1,0,0,0,0,0,\dots,0,\dots$$

formada solamente por cinco unos tiene por función generatriz la suma finita $F(x) = 1+x+x^2+x^3+x^4$, que también se puede escribir como el cociente de dos polinomios en la forma

$$F(x) = \frac{x^5-1}{x-1}$$

al tratarse de una progresión geométrica de razón x.

(c) Las siguientes dos funciones generatrices —o pequeñas variantes suyas— aparecen con cierta frecuencia, por lo que conviene tenerlas presentes:

(a) La función generatriz de la sucesión constante de término general $(a_k) = a$ para $k = 0,1,2,\dots$ es

$$F(x) = \frac{1}{1-ax}.$$

(b) La función generatriz de la sucesión de término general $(a_k) = k+1$ para $k = 0,1,2,\dots$ es

$$F(x) = \frac{1}{(1-x)^2}.$$

Las funciones generatrices son importantes como objetos combinatorios, ya que una serie de potencias formales $\sum_{k=0}^{\infty} a_k x^k$ puede codificar en sus coeficientes a_k cardinales de ciertos conjuntos, de forma que se utilizan como instrumento para muchos problemas de conteo. Veamos un ejemplo, esencialmente debido a Pólya, para entender precisamente de qué se trata.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Supongamos que queremos cambiar una moneda de 1 euro en monedas de céntimo, de las de curso legal actualmente; se tienen, por tanto, monedas de 1, 2, 5, 10, 20 y 50 céntimos.

Consideremos en primer lugar las monedas de 1 céntimo. Podríamos usar o bien ninguna, o bien una, o bien dos, o tres, o cuatro, etc.

$$\underline{0} \quad \underline{1} \quad \underline{1\ 1} \quad \underline{1\ 1\ 1} \quad \underline{1\ 1\ 1\ 1} \quad \cdots$$

Como mucho podríamos usar 100 para cambiar 1 euro. No limitaremos, sin embargo, su número, de manera que el razonamiento sirva para cantidades arbitrarias de euros.

Pero además tenemos monedas de 2 céntimos, y de 5, 10, 20 y 50, con las que el argumento anterior se puede repetir, y se obtienen "series"

$$\begin{array}{llllll}
\underline{0} & \underline{2} & \underline{2\ 2} & \underline{2\ 2\ 2} & \underline{2\ 2\ 2\ 2} & \cdots \\
\underline{0} & \underline{5} & \underline{5\ 5} & \underline{5\ 5\ 5} & \underline{5\ 5\ 5\ 5} & \cdots \\
\underline{0} & \underline{10} & \underline{10\ 10} & \underline{10\ 10\ 10} & \underline{10\ 10\ 10\ 10} & \cdots \\
\underline{0} & \underline{20} & \underline{20\ 20} & \underline{20\ 20\ 20} & \underline{20\ 20\ 20\ 20} & \cdots \\
\underline{0} & \underline{50} & \underline{50\ 50} & \underline{50\ 50\ 50} & \underline{50\ 50\ 50\ 50} & \cdots
\end{array}$$

Cambiar 1 euro significa entonces escoger un "montón" (los conjuntos de monedas subrayados) de cada una de las seis filas.

En cada fila, el hecho de poder elegir un elemento lo podemos representar como una "suma" (al fin y al cabo es la operación artimética más próxima a la disyunción):

$$\underline{0} + \underline{1} + \underline{1\ 1} + \underline{1\ 1\ 1} + \underline{1\ 1\ 1\ 1} + \cdots$$

Reservamos la "multiplicación" para representar el hecho de tomar "montones" de distintas filas:

$$(\underline{0} + \underline{1} + \underline{1\ 1} + \cdots) \cdot (\underline{0} + \underline{2} + \underline{2\ 2} + \cdots) \cdot (\underline{0} + \underline{5} + \underline{5\ 5} + \cdots) \cdots (\underline{0} + \underline{50} + \underline{50\ 50} + \cdots)$$

Al efectuar la multiplicación, cada sumando consta de 6 términos, uno por cada una de las filas de montones de monedas que representamos arriba. Es decir, cada sumando corresponde a una selección de monedas diferente.

Si representamos por un símbolo x al valor 1 céntimo, podemos establecer una representación algebraica obvia entre los "montones" de monedas y las potencias

de x, por ejemplo

$$\underline{1\ 1\ 1} = xxx = x^3$$
$$\underline{10\ 10} = x^{10}x^{10} = x^{20}$$
$$\underline{0} = x^0 = 1$$

Ahora podemos representar algebraicamente el producto anterior de sumas de "montones" de monedas como

$$\begin{aligned}(1+x+x^2+\cdots)\cdot\\ &\cdot(1+x^2+x^4+\cdots)\cdot\\ &\cdot(1+x^5+x^{10}+\cdots)\cdot\\ &\cdot(1+x^{10}+x^{20}+\cdots)\cdot\\ &\cdot(1+x^{20}+x^{40}+\cdots)\cdot\\ &\cdot(1+x^{50}+x^{100}+\cdots)\end{aligned}$$

Por ejemplo, uno de los términos en este producto es

$$x^3 \cdot 1 \cdot x^5 \cdot x^{10} \cdot 1 \cdot x^{50} = x^3 \cdot x^5 \cdot x^{10} \cdot x^{50},$$

que corresponde a la selección de 3 monedas de un céntimo, 1 moneda de 5 céntimos, ninguna moneda de dos céntimos, 1 moneda de diez céntimos, ninguna de veinte y 1 de cincuenta céntimos.

Este término del producto, es decir, esta selección de monedas, corresponde a un cambio de

$$3+5+10+50 = 68 \text{ céntimos}$$

en los tipos de monedas disponibles (lógicamente se suman los exponentes de las potencias de x).

El problema inicial no era contar las posibilidades de cambio de 68 céntimos, sino 100 céntimos (= 1 euro). Para contar *todas* basta entonces efectuar el producto y recoger los términos con la misma potencia de x, obteniendo una serie de potencias formal

$$a_0 + a_1x + a_2x^2 + \cdots + a_{68}x^{68} + \cdots + a_{100}x^{100} + \cdots$$

donde el coeficiente a_0 es el número de posibilidades de cambiar 0 céntimos, es decir, $a_0 = 1$, el coeficiente a_1 recoge las posibilidades que se tienen de cambiar 1 céntimo, es decir $a_1 = 1$, el coeficiente a_2 codifica las posibilidades de cambio de

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

dos céntimos, es decir, $a_2 = 2$, etc. El coeficiente a_{100} ofrece entonces la respuesta al problema inicial.

El problema se reduce a cómo calcular a_{100}. Este curso usaremos una sesión de prácticas ordenador para comprobar con el sistema de cálculo simbólico *Mathematica* que $a_{100} = 4562$.

Las funciones generatrices también encuentran su aplicación en la resolución de ecuaciones definidas de forma recurrente, que es el objeto de estudio del siguiente capítulo.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

[Aig] Aigner, M.: A course in enumeration. Springer, 2007

[BRV] Basart, J. M., Rifà, J., Villanueva, M.: Fonaments de matemàtica discreta. Elements de combinatòria i d'aritmètica. Universitat Autònoma de Barcelona, 1999

[Cab] Caballero Roldán, Rafael et al.: Matemática Discreta para Informáticos. Ejercicios resueltos. Pearson/Prentice Hall, 2007

[Conr] Conradie, W., Goranko, V.: Logic and Discrete Mathematics. A concise introduction. Wiley, 2015

[Fine] Fine, B. et al.: Geometry and discrete mathematics. De Gruyter, 2018

[HHM] Harris, J.M., Hirst, J.L., Mossinghoff, M.J.: Combinatorics and Graph Theory. Second edition. Springer, 2010

[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3. ed. McGraw Hill, 2007

[Mar] Martin, G.E.: Counting: the art of enumerative combinatorics. Springer, 2001

[PTW] Pólya, G., Tarjan, R.E., Woods, D.R.: Notes on introductory combinatorics. Birkhäuser, 2010

[Rib] Ríbnikov, K.: Análisis combinatorio. Mir Moscú, 1988

Capítulo 17. Ecuaciones en diferencias lineales y recursión

Un aspecto fundamental en Matemáticas es la resolución de ecuaciones. Estas ecuaciones adoptan diferentes formas y se resuelven con diferentes técnicas en función de la naturaleza de sus incógnitas. Por ejemplo, los sistemas de ecuaciones lineales de la escuela son conjuntos de ecuaciones polinómicas de grado uno y cuyas soluciones son números reales (elementos del cuerpo $\mathbb{R}$). Este es un caso muy fácil, cuya solución efectiva constituye el método de eliminación de Gauß. Otro caso algo más complicado son las ecuaciones diofánticas lineales en dos variables, cuyas soluciones se restringen al anillo de los números enteros.

En este capítulo consideraremos ecuaciones lineales cuyas incógnitas son sucesiones de números reales. La pregunta típica en este contexto es del estilo: ¿existe alguna sucesión —y si existe, calcularla— de números reales (a_n) de manera que para cualquier lugar n de la sucesión se verifique que

$$a_n = a_{n-1} + a_{n-2}?$$

Se trata, pues, de sucesiones definidas de forma *recurrente*.

Una primera respuesta trivial es la sucesión constante igual a 0. Pero hay más respuestas. Por ejemplo, la sucesión

$$1, 6, 7, 13, 21, 34, \ldots$$

… o la sucesión

$$3, 1, 4, 5, 9, 13, 22, \ldots$$

… o la sucesión de Fibonacci

$$1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$$

¡La solución no es única! De hecho, la suma (término a término) de dos sucesiones cualesquiera que tomemos que sean solución vuelve a ser una solución, y si tomamos una sucesión y la multiplicamos por un número real (término a término, de forma que todos los términos queden multiplicados por el mismo número), la sucesión resultante vuelve a ser solución. Esto, unido a que la sucesión constante

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

0 es solución, nos muestra que las sucesiones que son solución de la ecuación propuesta tienen estructura de subespacio vectorial dentro del $\mathbb{R}$-espacio vectorial de las sucesiones de números reales.

Se puede forzar la solución única: en el ejemplo basta fijar los dos primeros términos a_0 y a_1 de la sucesión dada. Por ejemplo, si $a_0 = a_1 = 1$, entonces la única solución que resuelve la ecuación

$$a_n = a_{n-1} + a_{n-2}$$

es la de Fibonacci. Precisamente el hecho de que la solución sea única cuando fijamos *dos* términos nos indica que el espacio vectorial real de las soluciones de la ecuación $a_n = a_{n-1} + a_{n-2}$ tiene dimensión 2 (aunque sea subespacio del espacio vectorial de todas las sucesiones de números reales, que es infinito-dimensional).

Justamente la estructura de espacio vectorial del conjunto de soluciones nos va a permitir la resolución, aunque hay formas alternativas de hacerlo. Las funciones generatrices son una herramienta muy útil en la resolución de ecuaciones en diferencias:

Ejemplo. Supongamos que queremos resolver

$$a_n = 5a_{n-1} + 3, \quad \text{para todo } n \geq 1$$

y con $a_0 = 1$.

La sucesión (a_n), cuyo término general queremos encontrar, puesto que es la respuesta al problema, posee una función generatriz de la forma

$$F(x) = \sum_{k=0}^{\infty} a_k x^k = a_0 + \sum_{k=1}^{\infty} a_k x^k.$$

Substituyendo los datos conocidos, que son $a_0 = 1$ y $a_k = 5a_{k-1} + 3$ para todo natural $k \geq 1$, queda

$$F(x) = 1 + \sum_{k=1}^{\infty} (5a_{k-1} + 3)x^k \iff F(x) - 1 = \sum_{k=1}^{\infty} (5a_{k-1} + 3)x^k.$$

Como

$$\sum_{k=1}^{\infty} (5a_{k-1} + 3)x^k = 5\sum_{k=1}^{\infty} a_{k-1}x^k + 3\sum_{k=1}^{\infty} x^k = 5x\sum_{k=1}^{\infty} a_{k-1}x^{k-1} + 3x\sum_{k=1}^{\infty} x^{k-1},$$

tras una reordenación del subíndice en $\sum_{k=1}^{\infty} a_{k-1}x^{k-1}$ resulta

$$F(x) - 1 = 5xF(x) + 3x\frac{1}{1-x} \iff (1-5x)F(x) = \frac{1+2x}{1-x},$$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

es decir, se obtiene que

$$F(x) = \frac{1+2x}{(1-x)(1-5x)}.$$

Apliquemos ahora el método de los coeficientes indeterminados para descomponer $F(x)$ en la suma

$$\begin{aligned}F(x) =& \frac{1+2x}{(1-x)(1-5x)}\\ =& \frac{A}{1-x} + \frac{B}{1-5x}\\ =& \frac{A(1-5x)+B(1-x)}{(1-x)(1-5x)}\\ =& \frac{(A+B)+(-5A-B)x}{(1-x)(1-5x)},\end{aligned}$$

que lleva a un sistema lineal de indeterminadas A y B compatible determinado, con solución $A = -3/4$ y $B = 7/4$. Esto quiere decir que

$$\begin{aligned}F(x) =& \frac{-3/4}{1-x} + \frac{7/4}{1-5x}\\ =& \frac{-3}{4}\sum_{k=0}^{\infty} x^k + \frac{7}{4}\sum_{k=0}^{\infty}(5x)^k\\ =& \sum_{k=0}^{\infty}\Big(\frac{-3}{4} + \frac{7}{4}\cdot 5^k\Big)x^k,\end{aligned}$$

de donde se sigue que el término general de la sucesión dada es

$$a_n = \frac{-3}{4} + \frac{7}{4}5^n.$$

Pero esta aplicación de las funciones generatrices a la resolución de ecuaciones en diferencias se puede entender como muy circunscrito a la facilidad de la ecuación propuesta. Un método definitivo es el que se apoya en la estructura de espacio vectorial del conjunto de soluciones de las ecuaciones en diferencias lineales.

Definición. Sea $N \in \mathbb{N}$, $N \geq 1$. Dada una sucesión $(a_n)_{n=0}^{\infty}$, una ecuación de la forma

$$a_{k+N} + \alpha_k^{[N-1]} a_{k+N-1} + \cdots + \alpha_k^{[0]} a_k = f_k,$$

donde $(\alpha_k^{[N-1]}), \ldots, (\alpha_k^{[0]})$ y (f_k) son sucesiones conocidas, se llama *ecuación en diferencias lineal*, o también, simplificando la expresión, *recurrencia lineal*, de orden N. Las sucesiones $(\alpha_k^{[N-1]}), \ldots, (\alpha_k^{[0]})$ se llaman *sucesiones de coeficientes* y la sucesión (f_k) recibe los nombres de *término independiente*, *término no homogéneo*

o también *término fuente*. Si el término fuente es la sucesión nula la ecuación en diferencias se llama *homogénea*, en caso contrario se llama *no homogénea* o a veces también *completa*. Una ecuación en diferencias lineal de orden N se dice que tiene *coeficientes constantes* si las sucesiones de coeficientes son sucesiones constantes.

En este curso nos centramos en la resolución de las ecuaciones en diferencias lineales con coeficientes constantes, por ser las más sencillas. Distinguiremos las ecuaciones homogéneas de las no homogéneas.

Solución general de la ecuación homogénea. Se trata de encontrar todas las soluciones de la ecuación en diferencias

$$a_{k+N} + \alpha^{[N-1]} a_{k+N-1} + \cdots + \alpha^{[0]} a_k = 0, \qquad (\dagger)$$

con $\alpha^{[N-1]}, \ldots, \alpha^{[0]}$ números reales. Para ello se supone que la solución, si existe, es una sucesión

$$(r^k), \text{ con } r \text{ un número complejo no nulo.}$$

Si es solución, deberá satisfacer la ecuación ($\dagger$), es decir, deberá cumplir que

$$r^{k+N} + \alpha^{[N-1]} r^{k+N-1} + \cdots + \alpha^{[0]} r_k = 0$$

para cada $k = 0, 1, 2, \ldots$, lo que son un número infinito de condiciones, pero que se reducen a una sola cuando se divide por r^k (esto, por cierto, es posible al ser $r \neq 0$), que es la igualdad

$$r^N + \alpha^{[N-1]} r^{N-1} + \cdots + \alpha^{[0]} = 0.$$

Se forma con ello el llamado *polinomio característico*

$$\rho(t) = t^N + \alpha^{[N-1]} t^{N-1} + \cdots + \alpha^{[0]},$$

de modo que cada una de sus raíces originan una sucesión (r^k) que es solución de la ecuación en diferencias propuesta. El polinomio característico puede tener todas sus raíces simples o tener raíces múltiples, y tener 0 como raíz; estos tres casos nos conducen a diferentes escenarios para el espacio de soluciones, como tratamos a continuación.

(i) *Si el polinomio característico tiene todas sus raíces simples:* Si $\rho(t)$ posee todas sus raíces $r_1, \ldots, r_N$ distintas y no nulas, entonces las N sucesiones

$$(r_1^k), (r_2^k), \ldots, (r_N^k)$$

son soluciones de la ecuación propuesta, y además son linealmente independientes; se demuestra que forman una base del espacio de soluciones, y, por tanto, la

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

solución más general de la ecuación (†) es de la forma

$$(A_1 r_1^k + A_2 r_2^k + \cdots + A_N r_N^k),$$

donde $A_1, \ldots, A_N$ son constantes.

Por ejemplo, el polinomio característico asociado a la ecuación en diferencias $a_{k+3} - 2a_{k+2} - 5a_{k+1} + 6a_k = 0$, con $k \in \mathbb{N}$, es $\rho(t) = t^3 - 2t^2 - 5t + 6$, que tiene como raíces 3, 1 y -2, todas ellas simples, es decir, de multiplicidad 1.

(ii) *Si el polinomio característico tiene raíces múltiples:* Supongamos que las raíces del polinomio característico $\rho(t)$ son

$$r_1, r_2, \ldots, r_M \ \text{ con } M < N,$$

distintas dos a dos y no nulas. Para cada $i = 1, \ldots, M$ supongamos que la raíz r_i tiene multiplicidad μ_i, es decir, se verifica la factorización

$$\rho(t) = (t - r_1)^{\mu_1} \cdot (t - r_2)^{\mu_2} \cdots (t - r_M)^{\mu_M}.$$

A cada raíz r_i del polinomio característico le corresponden las siguientes μ_i soluciones de la ecuación (†):

$$(r_i^k), (k r_i^k), (k^2 r_i^k), \ldots, (k^{\mu_i - 1} r_i^k).$$

Por tanto, una base del espacio de soluciones está formada por las μ_1 soluciones de este tipo que corresponden a la raíz r_1 unidas a las μ_2 soluciones de este tipo que corresponden a la raíz r_2 unidas a ..., unidas a las μ_M soluciones correspondientes a la raíz r_M del polinomio característico.

Por ejemplo, el polinomio característico asociado a la ecuación en diferencias $a_{k+4} - 3a_{k+3} - 3a_{k+2} + 7a_{k+1} + 6a_k = 0$, $k \in \mathbb{N}$ es $\rho(t) = t^4 - 3t^3 - 3t^2 + 7t + 6$, que tiene como raíces $r_1 = 3$, $r_2 = 2$ (simples, es decir, con $\mu_1 = \mu_2 = 1$) y $r_3 = -1$ (de multiplicidad $\mu_3 = 2$).

(iii) *Si cero es una raíz del polinomio característico:* El cero es raíz del polinomio característico si y solamente si $a^{[0]} = 0$ en la ecuación (†). Además, si 0 es una raíz del polinomio característico de multiplicidad μ, entonces hay μ soluciones de la forma

$$(1,0,0,0,\ldots), (0,1,0,0,\ldots), (0,0,1,0,\ldots), \ldots$$

Por ejemplo, la ecuación en diferencias $a_{k+2} - a_{k+1} = 0$ tiene asociado el polinomio característico $\rho(t) = t^2 - t$, cuyas raíces son $r_1 = 1$ y $r_2 = 0$ (simples).

Nota. A veces se pide solamente encontrar una solución particular de la ecuación homogénea. Esto tiene relación con el llamado *problema de valores iniciales*, que consiste en encontrar la única solución que existe de una ecuación en diferencias

lineal, de coeficientes constantes, de orden N cuando se imponen N condiciones iniciales, es decir, cuando se fijan N términos de la sucesión que se está buscando en el espacio de soluciones.

Ejemplo. Encontremos la solución general de la ecuación homogénea

$$a_k = 5a_{k-1} \iff a_k - 5a_{k-1} = 0.$$

El polinomio característico asociado es $\rho(t) = t - 5$, que posee una única raíz (simple) $t = 5$. Luego la solución general es de la forma

$$(A \cdot 5^k),\ k = 1, 2, \ldots \text{ con } A \text{ una constante.}$$

Si queremos encontrar la solución particular de esta ecuación homogénea cuando $a_0 = 1$, basta imponer esta condición en la solución general para encontrar la constante A adecuada:

$$\text{Para } k = 0 \text{ es } 1 = a_0 = A \cdot 5^0 \quad \iff \quad 1 = A \cdot 1,$$

es decir, $A = 1$ y la solución particular buscada es la sucesión

$$(5^k),\ k = 1, 2, \ldots$$

Solución general de la ecuación no homogénea. Se trata de resolver la ecuación

$$a_{k+N} + \alpha^{[N-1]} a_{k+N-1} + \cdots + \alpha^{[0]} a_k = f_k.$$

Se expresa como suma de la ecuación general de la ecuación homogénea asociada

$$a_{k+N} + \alpha^{[N-1]} a_{k+N-1} + \cdots + \alpha^{[0]} a_k = 0$$

(según el estudio anterior) más una solución particular de la no homogénea. El aspecto que puede presentar esta solución particular depende de qué tipo de sucesión sea el término fuente: si es una sucesión constante se probarán sucesiones constantes, si es una sucesión polinómica, es decir, de la forma

$$f_k = c_0 + c_1 k + c_2 k^2 + \cdots + c_n k^n,$$

se ensayarán soluciones particulares de este tipo.

Ejemplo. Encontremos la solución general de la ecuación no homogénea

$$a_k = 5a_{k-1} + 3.$$

Sabemos que la solución general de la ecuación no homogénea es suma de la solución de la ecuación general de la ecuación homogénea asociada más una solución particular de la no homogénea.

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

La solución general de la ecuación homogénea asociada la hemos calculado en el ejemplo anterior, y es

$$(A \cdot 5^k), \text{ con } A \text{ constante.}$$

Para encontrar una solución particular de la ecuación no homogénea, como el término fuente es constante, probamos una sucesión constante, digamos de término general

$$f_k = \beta.$$

Por tanto, si esta sucesión es solución de la ecuación $a_k = 5a_{k-1} + 3$, ha de satisfacerla, esto es, ha de verificarse que

$$\beta = 5\beta + 3 \longleftrightarrow \beta - 5\beta = 3 \Longleftrightarrow -4\beta = 3 \Longleftrightarrow \beta = -\frac{3}{4},$$

luego la solución general buscada es

$$\left(A \cdot 5^k - \frac{3}{4}\right),\ k = 1, 2, \ldots \text{ con } A \text{ constante.}$$

Si nos pidieran la solución de la ecuación propuesta con condición inicial $a_0 = 1$, entonces bastaría —como antes— imponer esta condición en la solución general:

$$A \cdot 5^0 - \frac{3}{4} = 1 \Longleftrightarrow A - \frac{3}{4} = 1 \Longrightarrow A = 1 + \frac{3}{4} = \frac{7}{4},$$

y así la solución buscada es

$$\left(\frac{7}{4} \cdot 5^k - \frac{3}{4}\right),\ k = 1, 2, \ldots$$

Obsérvese que la solución coincide con la encontrada aplicando nuestros conocimientos sobre funciones generatrices al principio del capítulo.

A veces el término fuente es distinto al esperado, como cuando tomamos una ecuación como la del ejemplo anterior pero cuyo polinomio característico tiene 1 como raíz:

Ejemplo. Encontremos la solución general de la ecuación no homogénea

$$a_k = a_{k-1} + 3.$$

La solución general de la ecuación no homogénea es suma de la solución de la ecuación general de la ecuación homogénea asociada más una solución particular de la no homogénea.

La solución general de la ecuación homogénea asociada es la sucesión constante

$$(A \cdot 1^k) = (A, A, A, A, \ldots) \text{ con } A \in \mathbb{R}.$$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Para encontrar una solución particular de la ecuación no homogénea, como el término fuente es constante, tenderíamos a ensayar como solución una sucesión constante, digamos $f_k = \beta$; pero esto nos llevaría esta vez a $\beta = \beta + 3$, es decir, $0 = 3$, lo cual es absurdo. En este caso hemos de ensayar una solución particular polinómica de tipo

$$f_k = c_0 + c_1 k.$$

Esta sucesión, si es solución de la ecuación propuesta, ha de satisfacerla, es decir, ha de cumplir $f_{k+1} = f_k + 3$, i.e., $c_0 + c_1(k+1) = c_0 + c_1 k + 3$. Un sencillo análisis nos lleva a tomar los valores $c_0 = 0$ y $c_1 = 3$ y, por tanto, a proponer como solución particular la sucesión

$$f_k = 0 + 3k = 3k, \quad k = 1, 2, \ldots$$

La solución general de la ecuación propuesta es

$$\Big(A + 3k\Big), \ k = 1, 2, \ldots \ \text{ con } A \text{ constante.}$$

Si nos pidieran la solución de la ecuación propuesta con condición inicial $a_0 = 1$, entonces bastaría —como antes— imponer esta condición en la solución general:

$$A + 3 \cdot 0 = 1 \Longleftrightarrow A + 0 = 1 \Longrightarrow A = 1,$$

y así la solución buscada es

$$\Big(1 + 3k\Big), \quad k = 1, 2, \ldots$$

En las prácticas con el programa *Mathematica* del laboratorio informático de esta asignatura se verán muchos más ejemplos, así como su resolución por medio del mencionado *software*. Todos los detalles, incluidas las demostraciones —que se han omitido a lo largo de este capítulo— pueden ser consultados por ejemplo en el capítulo 8 de [**SS**].

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

[BRV] Basart, J. M., Rifà, J., Villanueva, M.: Fonaments de matemàtica discreta. Elements de combinatòria i d'aritmètica. Universitat Autònoma de Barcelona, 1999

[Big] Biggs, N.L.: Discrete Mathematics. Second ed. Oxford U.P., 2004

[Conr] Conradie, W., Goranko, V.: Logic and Discrete Mathematics. A concise introduction. Wiley, 2015

[FG] Ferrando, J.C., Gregori, V.: Matemática Discreta. 2. ed. Reverté, 2002

[GOV] Galindo Pastor, C., Orús Báguena, M.P., Vindel Cañas, M.P.: Problemes de matemàtica discreta. Universitat Jaume I, 1997

[Gall] Gallier, J.: Discrete Mathematics. Springer, 2011

[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3. ed. McGraw Hill, 2007

[Rios] Ríos, S.: Matemática finita. Paraninfo, 1974

[SS] Sanz-Serna, J.M.: Diez lecciones de cálculo numérico. Universidad de Valladolid, 1998

[Wall2] Wallis, W.D.: A beginner's guide to discrete mathematics. Second edition. Birkhäuser, 2012

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Capítulo 18. Conceptos básicos de teoría de grafos

Sin entrar en mucho detalle, un *grafo* es un sistema de nodos y aristas que los unen, es decir, una red de carreteras abstracta. Queremos estudiar en este curso grafos cuyas aristas no marcan sentido alguno, o, en la analogía con la red de carreteras, que no poseen pistas de sentido único. (Los grafos que reflejan el sentido de las aristas reciben el nombre de grafos dirigidos o digrafos.)

Para poder definir en general la noción de grafo sin direcciones, introducimos la siguiente notación para un conjunto V:

$$V^{(2)} := \{U \subseteq V : 1 \leq |U| \leq 2\};$$

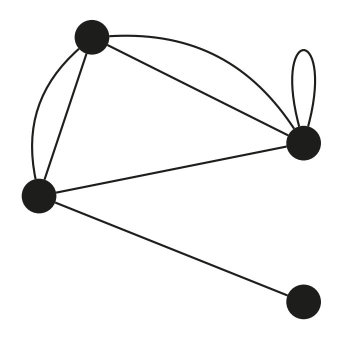
esto es, $V^{(2)}$ es el conjunto de los subconjuntos de V que poseen por lo menos un elemento y a lo sumo dos.

Definición. Un *grafo* (no dirigido) es una terna $G = (V, E, i)$, donde

(a) V es un conjunto cuyos elementos se llaman *vértices* del grafo G;
(b) E es un conjunto disjunto con V cuyos elementos se llaman *aristas* de G;
(c) $i : E \longrightarrow V^{(2)}$ es una aplicación.

Observemos la figura de la derecha. En este ejemplo hemos representado los vértices como puntos en el plano y las aristas como segmentos o caminos que conectan vértices. Hay dos tipos de vértices:

(i) aristas ordinarias, que son aquellas aristas e tales que $i(e) = \{x, y\}$ para $x, y \in V$ con $x \neq y$;
(ii) lazos, que son las aristas para las que $i(e) \in V$.



Las aristas ordinarias unen dos vértices distintos, llamados *extremos* de la arista. Un lazo une un vértice consigo mismo. Dos vértices se llaman *adyacentes* o *vecinos* si están unidos por una arista. Los vértices pueden estar conectados por más de

ISBN: 978-84-17900-65-6

DOI: http://dx.doi.org/10.6035/Sapientia170

una arista, y entonces se dice que el grafo contiene aristas múltiples (puede haber también lazos múltiples).

Los grafos que no tienen ni aristas múltiples ni lazos (tanto simples como múltiples) se denominan *simples*. En adelante escribiremos grafo queriendo decir grafo simple, a menos que indiquemos lo contrario. Igualmente restringiremos el estudio a grafos *finitos*, es decir, aquellos con un número finito de vértices y aristas.

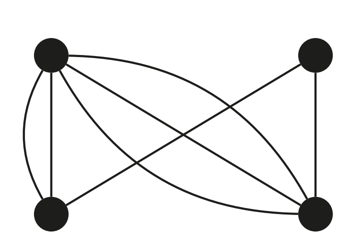
En los grafos simples cada arista queda unívocamente determinada por sus extremos. Así se puede simplificar el modelo abstracto y definir el conjunto de aristas E como un subconjunto cualquiera de

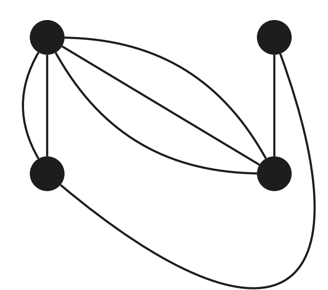
$$\Big\{\{x,y\} : x,y \in V, x \neq y\Big\}.$$

Con frecuencia escribiremos xy en vez de $\{x,y\}$ para la arista que une los vértices x e y. Un grafo simple se compone tanto de un conjunto de vértices V como de un subconjunto E de $\Big\{\{x,y\} : x,y \in V, x \neq y\Big\}$. Se expresa entonces diciendo "sea $G = (V,E)$ un grafo", o también "el conjunto de vértices resp. de aristas de G se denota como $V(G)$ resp. $E(G)$".

Hay que distinguir entre un grafo y su representación gráfica: un mismo grafo se puede dibujar de maneras distintas.

Ejemplo. Las dos siguientes representaciones corresponden al mismo grafo:





Por otro lado, grafos distintos que poseen propiedades esenciales comunes se denominan *isomorfos*:

Definición. Sean $G = (V,E), \tilde{G} = (\tilde{V},\tilde{E})$ dos grafos (no necesariamente simples). Un *isomorfismo* de G en $\tilde{G}$ es un par de aplicaciones (φ,ψ) donde $\varphi : V \to \tilde{V}$ y

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

$\psi : E \to \tilde{E}$ son biyecciones tales que para todo $e \in E$ si sus extremos son x e y entonces los extremos de $\psi(e)$ son $\varphi(x)$ y $\varphi(y)$.

En particular, dos grafos isomorfos se pueden representar por el mismo dibujo.

Una forma práctica de saber si dos grafos son isomorfos consiste en estudiar su matriz de adyacencia:

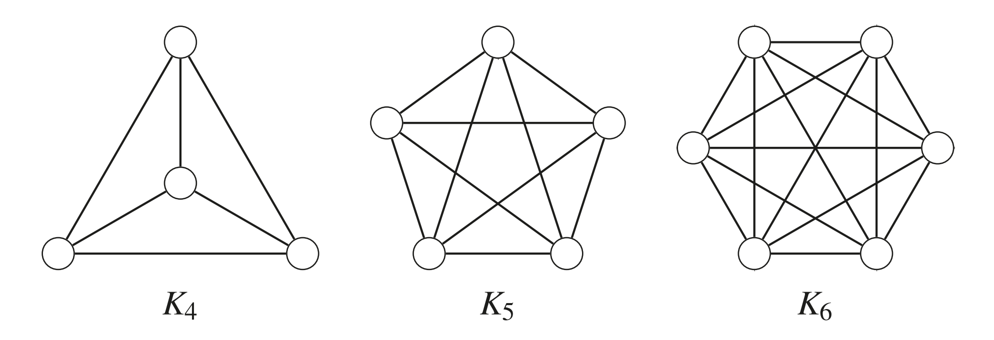
Definición. Sea $G = (V,E)$ un grafo no necesariamente simple con $V = \{v_1,\dots,v_n\}$. La *matriz de adyacencia* de G es una matriz $M = (m_{ij})$, $1 \leq i, j \leq n$, cuya entrada (i, j) es el número de aristas que unen v_i y v_j.

La matriz de adyacencia de un grafo es una matriz simétrica. En el caso de grafos simples, las entradas de la diagonal son 0's y el resto son 0's ó 1's. Es relativamente sencillo demostrar (y se deja como ejercicio al lector):

Teorema 18.1. *Dos grafos G y $\tilde{G}$ son isomorfos si y solamente si existe una ordenación de los vértices de G y $\tilde{G}$ tal que las matrices de adyacencia de ambos coinciden.*

¡Nótese que no se dice que las matrices de adyacencia de ambos han de coincidir, sino que se pueden permutar sus filas y columnas de manera que sean la misma!

Una familia importante de ejemplos son los grafos completos K_n, que son aquellos grafos que tienen n vértices y todos ellos están unidos mediante una arista a todos los demás:



K_4 K_5 K_6

Mientras que una arista de un grafo (simple) tiene exactamente dos extremos, en un vértice puede confluir un número cualquiera de aristas.

Definición. Sea $G = (V,E)$ un grafo, sea v un vértice de G. El número

$$\gamma(v) := \{e \in E : e \text{ termina en } v\}$$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

se denomina *índice de adyacencia* o *grado* de v.

Una primera observación es:

Teorema 18.2 (Lema del “handshaking”)**.** *Se verifica que*

$$\sum_{v\in V} \gamma(v) = 2\cdot |E|.$$

Es evidente, pues cada arista se cuenta dos veces, una por cada uno de sus dos extremos. (Este teorema también es válido para grafos que no son simples si contamos los lazos en sus respectivos vértices con grado 2.)

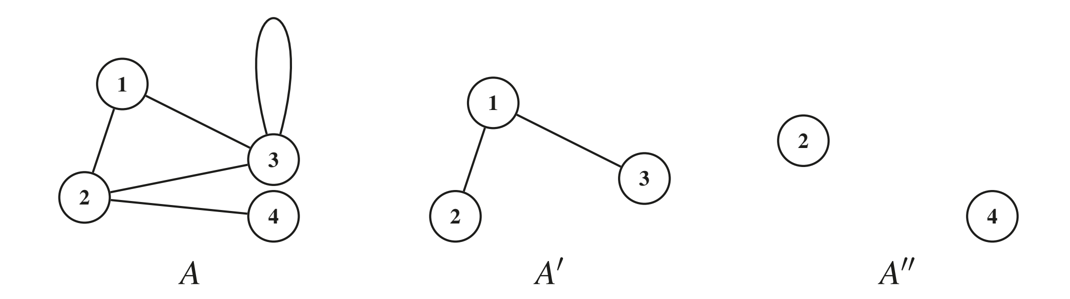
Definición. Sean $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$ dos grafos. Si $V_1 \subseteq V_2$ y $E_1 \subseteq E_2$ se dice que G_1 es un *subgrafo* de G_2. En el caso en que $V_1 = V_2$ se dice que G_1 es un *subgrafo generador* de G_2. Si

$$E_1 = \{e \in E_2 : e \text{ une vértices } v, w \in V_1\}$$

entonces G_1 se llama *subgrafo inducido* por V_1.

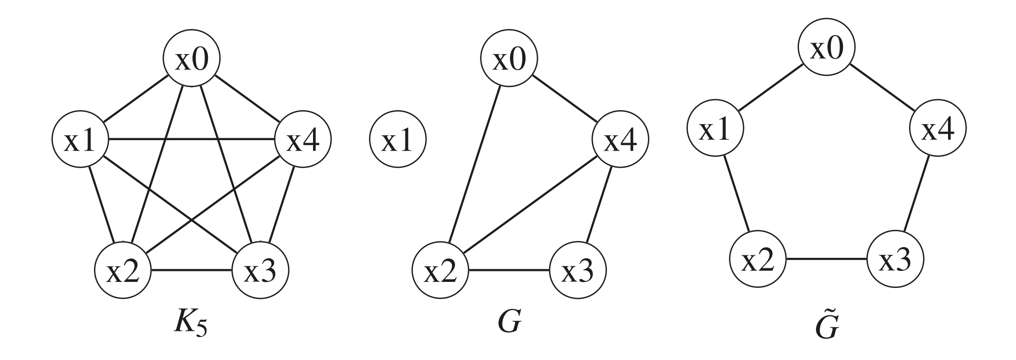
Dicho de otra manera: un subgrafo inducido consta de un subconjunto del conjunto de vértices y de todas las aristas que unen los vértices de este subconjunto.

Ejemplo. En la figura siguiente, los grafos A' y A'' son subgrafos del grafo A.

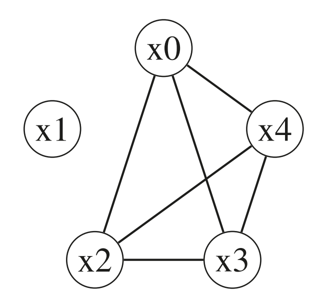


Ejemplo. Dado el grafo completo K_5, representamos a su derecha un subgrafo suyo $G = (V, E)$ con $V(G) = \{x_0, x_2, x_3, x_4\}$ (el vértice x_1 se representa para resaltar la comparación con K_5, pero no es vértice del grafo G), que no es generador, ya que $V(K_5) \neq V(G)$. Sin embargo, el grafo $\tilde{G}$ sí es un subgrafo generador de K_5:

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170



El siguiente grafo es el subgrafo de K_5 inducido (o generado) por $\{x_1, x_2, x_3, x_4\}$:



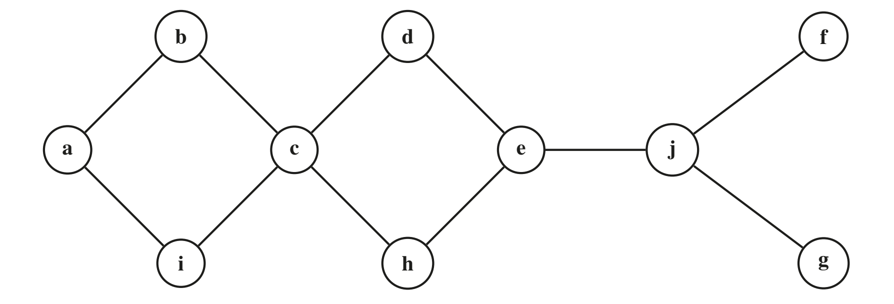
En una red de carreteras ha de poder encontrarse un "camino" si se quiere llegar de una localidad a otra. Precisemos este y otros conceptos.

Sea $G = (V, E)$ un grafo. Una sucesión $x_0, \ldots, x_n$ de vértices es una *trayectoria* si $\{x_i, x_{i+1}\}$ para $i = 0, 1, \ldots, n-1$ es una arista de G. En el caso en que $x_0 \neq x_n$ se habla de trayectoria *abierta*, en otro caso *cerrada*. Una trayectoria $x_0, x_1, \ldots, x_n$ se dice que tiene *longitud n*. El vértice x_0 se llama inicial, y el vértice x_n se llama final de la trayectoria; en tal caso se dice que la trayectoria une x_0 y x_n.

Una trayectoria se llama *camino* si contiene cada arista a lo sumo una vez. Un camino es un *camino simple* si contiene cada vértice x_i, $i \neq 0$, $i \neq n$ a lo sumo una vez. (Si no se repiten vértices, no se pueden repetir aristas, pues una arista determina sus extremos.) Un camino simple cerrado se llama *ciclo* de G.

Ejemplo. Consideremos el grafo G de la figura:

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170



Una trayectoria en G es $bcicd$: no es un camino, pues se repite la arista ci. Una trayectoria cerrada es $bcicdcb$.

Un camino es, por ejemplo, $abcdehci$ (que no es camino simple, al repetirse el vértice c). Un circuito es $abcdehcia$. Un camino simple en G es $abcdeh$. Por último, es fácil identificar un ciclo en G, por ejemplo $abcia$.

Si $x_0, \ldots, x_n$ e $y_0, \ldots, y_m$ son trayectorias con $x_n = y_0$, se pueden componer para formar la sucesión

$$x_0, \ldots, x_n, y_1, \ldots, y_m.$$

Aunque ambas sean caminos simples, su composición no tiene por qué serlo. Además, de manera trivial se verifica:

Teorema 18.3. *Todo camino de x_0 a x_n puede acortarse a un camino simple de x_0 a x_n eliminando vértices.*

Definición. Sean x e y vértices de un grafo G que están unidos por al menos un camino simple. La *distancia* entre x e y es la longitud del camino simple más corto entre x e y. Se denota por $d(x,y)$.

Evidentemente $d(x,x) = 0$. Por convenio, si no existiera ningún camino simple de x a y se escribe $d(x,y) = \infty$.

La distancia nos permite hacer ciertas particiones del conjunto de vértices de un grafo $G = (V,E)$: para $x \in V$, sea $K(x) := \{y \in V : d(x,y) < \infty\}$. Entonces:

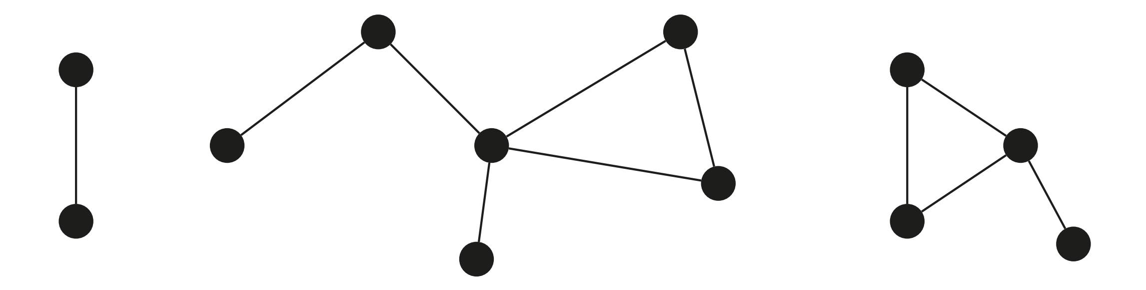
Teorema 18.4. *Para cualesquiera dos vértices $x, y \in V$ se tiene que o bien $K(x) = K(y)$ o bien $K(x) \cap K(y) = \varnothing$.*

Demostración. Tenemos que probar que $K(x) \cap K(y) \neq \varnothing$ implica $K(x) = K(y)$. Bastará mostrar que $K(x) \subseteq K(y)$, pues la contención contraria se prueba de manera análoga. Sean para ello $v \in K(y)$ y $w \in K(x) \cap K(y)$; entonces existen caminos simples de v a y, de y a w y de w a x. Si los componemos, obtenemos una trayectoria

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

de v a x (la composición no tiene por qué ser un camino simple, pero se puede acortar a uno tal). □

Así, es claro que los conjuntos $K(x)$ forman una partición (por tanto, ¡disjunta!) de V. Los subgrafos inducidos por los $K(x)$ se llaman *componentes conexas* de G. Por ejemplo, el grafo



posee 3 componentes conexas.

Definición. Un grafo se llama *conexo* si $d(x,y) < \infty$ para todo $x,y \in V$.

Ser conexo es equivalente a decir que $K(v) = V$ para todo $v \in V$.

Los vértices y aristas que hacen descomponer un grafo son interesantes:

Definición. Un vértice v se llama *articulación* de $G = (V,E)$ si el subgrafo inducido por $V \setminus \{v\}$ tiene más componentes conexas que G. Una arista $e \in E$ se denomina *puente* de V si el grafo $(V, E \setminus \{e\})$ tiene más componentes conexas que G.

El vértice azul de la figura es una articulación y la arista roja es una arista puente:



Teorema 18.5. *Sea G un grafo conexo con por lo menos dos vértices. Entonces posee dos vértices que no son articulaciones de G.*

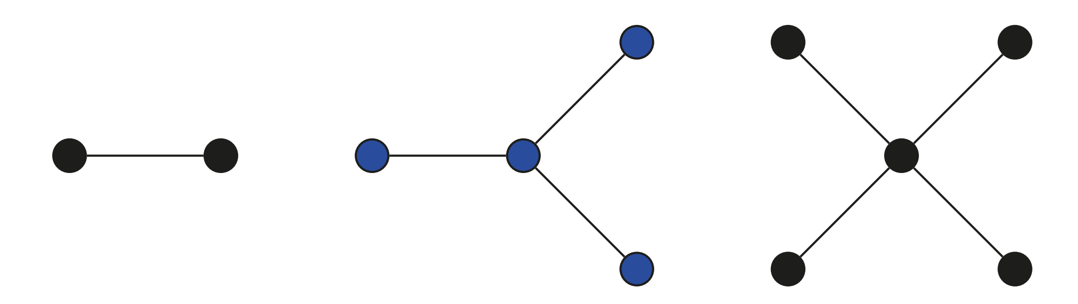
Demostración. La idea es escoger vértices x,y distintos de G que estén a distancia máxima. Los detalles se dejan al lector interesado. □

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Teorema 18.6. *Sea $G = (V,E)$ un grafo conexo. Entonces G posee por lo menos $|V| - 1$ aristas.*

Demostración. Se prueba por inducción sobre $|V|$. Para $|V| = 1$ no hay nada que probar. Por el Teorema 18.5 existe $v \in V$ que no es articulación. Por hipótesis de inducción, el subgrafo inducido por $V \setminus \{v\}$ posee a lo sumo $|V| - 2$ aristas, y así G ha de tener por lo menos una arista más que se conecte a v, lo que termina la prueba. □

En el Teorema 18.6 no cabe mejora alguna: ejemplo de ello son los grafos



Los grafos conexos con exactamente $|V| - 1$ aristas se denominan *árboles*, y son el objeto de estudio del capítulo siguiente.

ISBN: 978-84-17900-65-6

DOI: http://dx.doi.org/10.6035/Sapientia170

[Bas] Basart i Muñoz, J.M.: Grafs: fonaments i algorismes. Universitat Autònoma de Barcelona, Servei de Publicacions, 1998

[Big] Biggs, N.L.: Discrete Mathematics. Second ed. Oxford U.P., 2004

[Cab] Caballero Roldán, Rafael et al.: Matemática Discreta para Informáticos. Ejercicios resueltos. Pearson/Prentice Hall, 2007

[Conr] Conradie, W., Goranko, V.: Logic and Discrete Mathematics. A concise introduction. Wiley, 2015

[FG] Ferrando, J.C., Gregori, V.: Matemática Discreta. 2. ed. Reverté, 2002

[Gall] Gallier, J.: Discrete Mathematics. Springer, 2011

[HHM] Harris, J.M., Hirst, J.L., Mossinghoff, M.J.: Combinatorics and Graph Theory. Second edition. Springer, 2010

[Laf] Laforest, Ch.: À la découverte des graphes et des algorithmes de graphes. EDP Sciences, 2017.

[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3. ed. McGraw Hill, 2007

[Ore] Ore, ∅.: Graphentheorie und ihre Anwendungen. Klett, 1974

[Trias] Trias Pairó, J.: Matemàtica discreta. Problemes resolts. Universitat Politècnica de Catalunya, 2009

[Wall] Wallis, W.D.: A beginner's guide to graph theory. Second edition. Birkhäuser, 2007

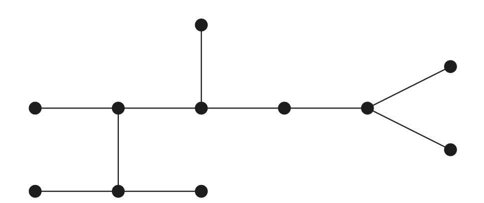
[Wall2] Wallis, W.D.: A beginner's guide to discrete mathematics. Second edition. Birkhäuser, 2012

[Wes] West, D.B.: Introduction to graph theory. Second edition. Prentice Hall, 2001

[Wil] Wilson, R.J.: Introduction to graph theory. Longman, 2010

Capítulo 19.
Árboles y grafos bipartitos

No se trata de silvicultura, pero: Un grafo sin ciclos se llama *bosque*; un grafo conexo sin ciclos se llama *árbol*. Por ejemplo:



Los árboles se pueden caracterizar mediante muchas propiedades:

Teorema 19.1. *Sea $G = (V,E)$ un grafo. Los siguientes asertos son equivalentes:*

(1) *G es un árbol.*
(2) *Cualesquiera dos vértices x,y de G están unidos mediante exactamente un camino simple.*
(3) *G es conexo y toda arista es un puente.*
(4) *G es conexo y $|E| = |V| - 1$.*
(5) *G no tiene ciclos y $|E| = |V| - 1$.*
(6) *G no tiene ciclos, pero si se unen dos vértices de G que no están unidos por una arista de G, entonces aparece exactamente un ciclo.*

Demostración.

$(1) \Rightarrow (2)$: Si hubiera dos caminos de x a y, existiría un ciclo en G, lo cual es imposible al ser un árbol.

$(2) \Rightarrow (3)$: G es conexo, cada arista es puente ya que cada uno de sus extremos no pueden estar conectados.

$(3) \Rightarrow (4)$: Se demuestra por inducción sobre $n = |V|$. Para $n = 1,2$ el aserto es trivial. Supongamos que es cierto para todo grafo G' con $V(G') < n$. Elegimos una arista $e \in E$. El grafo $G \setminus \{e\}$ descompone en exactamente dos componentes conexas G_1, G_2. Estas satisfacen de nuevo (3) y por la hipótesis de

ISBN: 978-84-17900-65-6

DOI: http://dx.doi.org/10.6035/Sapientia170

inducción se verifica $|E(G_i)| = |V(G_i)| - 1$ para $i = 1,2$. En suma, se tiene que

$$|E| = |E(G_1)| + |E(G_2)| + 1 = |V(G)| - 1$$

(donde el $+1$ corresponde a la arista e).

$(4) \Rightarrow (5)$: Si G posee un ciclo, entonces existe una arista e que no es un puente. Así se cumple por un lado que $G \setminus \{e\}$ es conexo, y por otro que $G \setminus \{e\}$ tiene $|G| - 2$ aristas, lo que es absurdo por el Teorema 18.6.

$(5) \Rightarrow (6)$: Supongamos que se verifica (5), entonces G no posee un ciclo, y así cada componente $G_1, G_2, \ldots, G_s$ de G es un árbol. Se tiene que

$$|E| = \sum_r |E(G_r)| \overset{(4)}{=} \sum_r (|V(G_r)| - 1) = |V| - r,$$

de donde se deduce que $r = 1$ y, por tanto, G es conexo. Sean además $x, y \in V$ dos vértices que no son adyacentes en G. Como G es conexo, existe un camino simple de x a y. Añadiendo una arista de x a y se creará un ciclo C_1. Si se creara un segundo ciclo C_2, poseería este una arista e' que no pertenecería a C_1. La eliminación de e' llevaría a un grafo que verifica (4). Por la implicación $(4) \Rightarrow (5)$, tal grafo no poseería ciclo alguno, ¡contradicción!

$(6) \Rightarrow (1)$: Una arista que une dos componentes no puede estar en un ciclo.

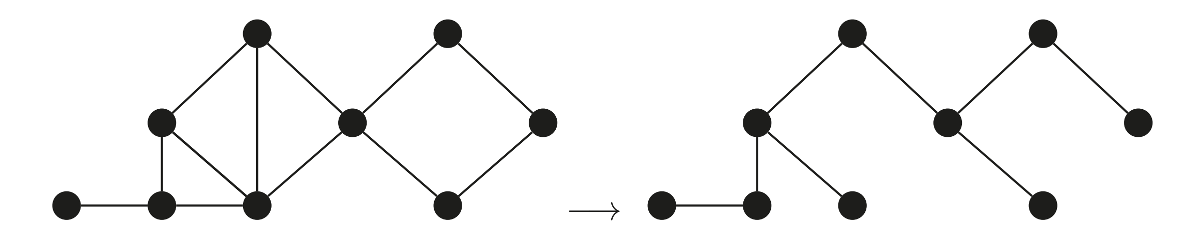
□

Del enunciado (4) se deduce inmediatamente:

Teorema 19.2. *Todo árbol posee por lo menos dos extremos.*

Consideremos ahora ciertos subgrafos distinguidos de un grafo G:

Definición. Si un subgrafo H de G es un árbol que contiene todos los vértices de G, entonces H se llama el *armazón* o *árbol generador* de G.



Teorema 19.3. *Un grafo G posee un árbol generador H si y solamente si es conexo.*

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Demostración. Si H es conexo, entonces G también lo es. Recíprocamente, supongamos que G es conexo; entonces se pueden ir eliminando sucesivamente todos los ciclos de G hasta que quede un árbol generador. Para ello han de eliminarse necesariamente

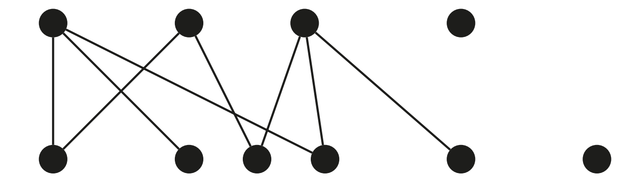
$$|E|-|V|+1$$

aristas, puesto que cada árbol generador H de G posee $|V|-1$ aristas. □

Existe una clase de grafos ligeramente mayor (como asegurará el Teorema 19.4) que los árboles: los grafos bipartitos.

Definición. Un grafo G se llama *bipartito* si el conjunto de sus vértices se puede descomponer en dos conjuntos disjuntos V_1 y V_2 tales que vértices de un mismo subconjunto no son adyacentes.

Un ejemplo de grafo bipartito es el de la figura:



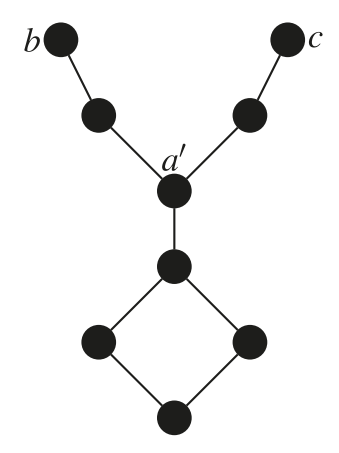
Los grafos bipartitos se caracterizan por sus ciclos:

Teorema 19.4. *Un grafo G es bipartito si y solamente si no contiene ciclos de longitud impar.*

Demostración. Supongamos en primer lugar que G fuera bipartito. En un ciclo tienen que aparecer alternativamente vértices de V_1 y V_2, por lo que el ciclo ha de tener longitud par.

Recíprocamente, es trivial que un grafo es bipartito si y solamente si cada una de sus componentes conexas lo es; por ello se puede suponer que G es conexo. Fijemos un vértice $a \in V$. Vamos a mostrar que si $d(a,b)=d(a,c)$, entonces b y c no son adyacentes. Para ello, sean W_1 y W_2 los caminos más cortos de a a b y de a a c, respectivamente. Sea a' el último vértice común a W_1 y W_2 anterior a b:

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170



Entonces los segmentos de a' a b y de a' a c forman un camino de longitud par de b a c. Esto significa que b y c no son adyacentes, pues de lo contrario tendríamos un ciclo de longitud impar. Por consiguiente, para vértices adyacentes b y c se tiene que $d(a,b) = d(a,c) \pm 1$. Los conjuntos

$$V_1 := \{b : d(a,b) \text{ par}\} \text{ y } V_2 := \{c : d(a,c) \text{ impar}\}$$

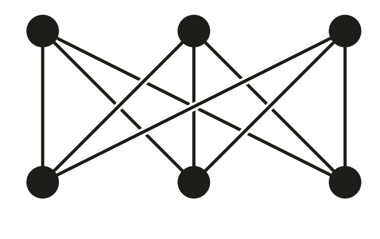
nos proporcionan la descomposición buscada. □

Como consecuencia se verifica:

Teorema 19.5. *Todo árbol es un grafo bipartito.*

El recíproco no es cierto, es decir, no todo grafo bipartito es un árbol (¿Puede dar un ejemplo?)

Por cierto, existe una familia de grafos bipartitos distinguida: la de aquellos en los que todos los vértices de un subconjunto de la partición son adyacentes a todos los de la otra. Se llaman grafos bipartitos completos y se denotan $K_{n,m}$ con $n \leq m$ si n y m son el número de vértices de cada una de las dos particiones.



$K_{3,3}$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

En el capítulo 22, en el que tratamos una generalización del concepto de grafo (en la que asignamos unas ciertas etiquetas o *pesos* a las aristas), describimos un algoritmo de cálculo de árboles generadores de peso mínimo, con múltiples aplicaciones prácticas. Pero antes queremos terminar el tema de los grafos bipartitos considerando el concepto de *emparejamiento*. En general:

Definición. Un *emparejamiento* de un grafo $G = (V,E)$ es un subconjunto E' de E tal que todas las aristas en E' son disjuntas dos a dos.

Sea $G = (V,E)$ un grafo bipartito, con $V = U \cup W$ la descomposición del conjunto de vértices: ni los vértices de U ni los de W están unidos entre ellos. Estamos interesados en determinar bajo qué condiciones existen emparejamientos de G. El resultado que nos responde tal cuestión recibe el nombre de teorema del matrimonio (o también teorema de Hall[1]). Para explicar el teorema y su sugestivo nombre, consideremos el conjunto U como una colección de señoras y el conjunto W como una colección de caballeros. Las aristas del grafo representan los afectos entre sexos. Cada una de las señoras quiere elegir un compañero dentro del círculo de sus admiradores (o admiradoras), estando prohibida la bigamia. Tal elección representa un emparejamiento E' con $|E'| = |U|$. Sea $N(U')$ el conjunto de los vecinos del subconjunto $U' \subseteq U$, es decir, el conjunto

$$W' = \{w : \text{existe un } u \in U' \text{ con } uw \in E\}.$$

Está claro que un emparejamiento E' con $|E'| = |U|$ solamente se puede hacer si para cada subconjunto $U' \subseteq U$ el conjunto de los admiradores $N(U')$ verifica la condición

$$|N(U')| \geq |N(U)|.$$

Si no, no habría suficientes candidatos a maridos para las señoras en U' y por lo menos una de ellas se quedaría con las ganas (le darían calabazas, como se decía antes).

La condición anterior no solamente es necesaria, sino también suficiente, como asegura el teorema:

Teorema 19.6 (Teorema del matrimonio)**.** *Sea $G = (V,E)$ un grafo bipartito con descomposición $V = U \cup W$ del conjunto de vértices. Existe un emparejamiento $E' \subseteq E$ con $|E'| = |U|$ si y solamente si $|N(U')| \geq |U'|$ para todo $U' \subset U$.*

Omitimos en este curso la demostración del Teorema 19.6.

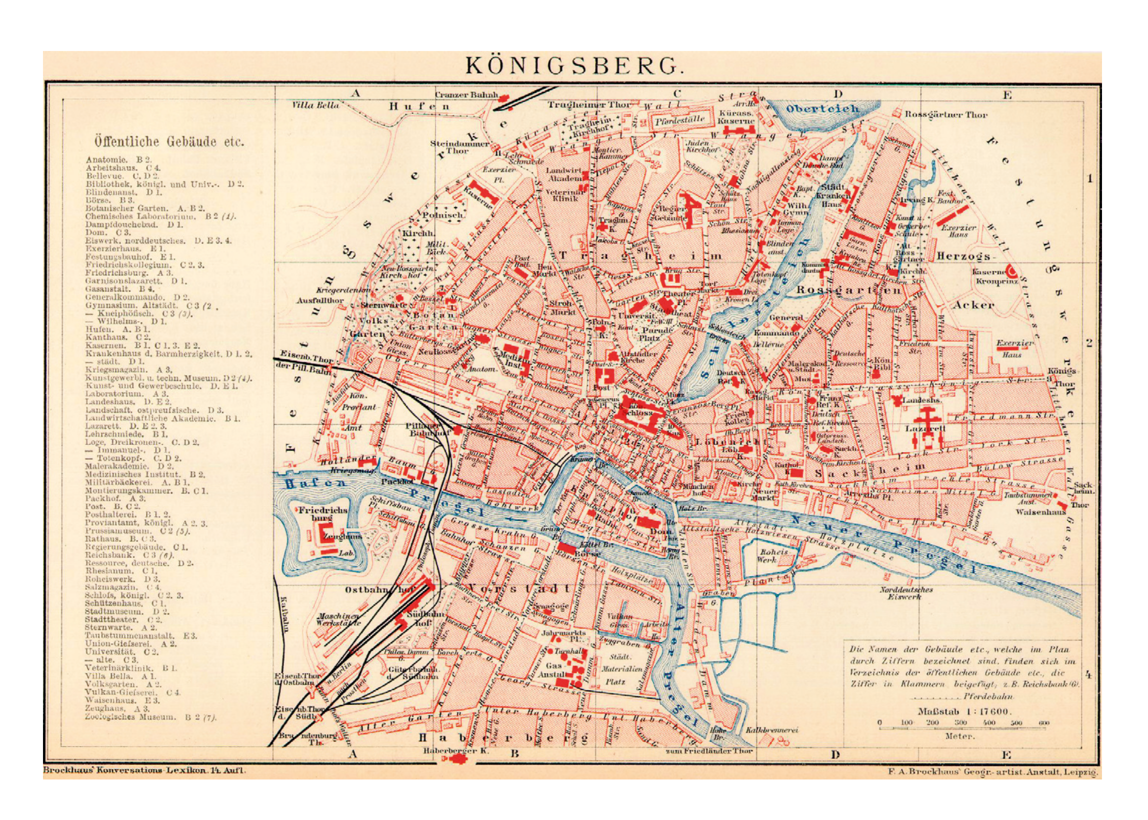
[1]Por el matemático inglés Philip HALL (1904–1982).

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

[Bas] Basart i Muñoz, J.M.: Grafs: fonaments i algorismes. Universitat Autònoma de Barcelona, Servei de Publicacions, 1998
[Big] Biggs, N.L.: Discrete Mathematics. Second ed. Oxford U.P., 2004
[Cab] Caballero Roldán, Rafael et al.: Matemática Discreta para Informáticos. Ejercicios resueltos. Pearson/Prentice Hall, 2007
[Conr] Conradie, W., Goranko, V.: Logic and Discrete Mathematics. A concise introduction. Wiley, 2015
[Gall] Gallier, J.: Discrete Mathematics. Springer, 2011
[HHM] Harris, J.M., Hirst, J.L., Mossinghoff, M.J.: Combinatorics and Graph Theory. Second edition. Springer, 2010
[Laf] Laforest, Ch.: À la découverte des graphes et des algorithmes de graphes. EDP Sciences, 2017.
[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3. ed. McGraw Hill, 2007
[Ore] Ore, ∅.: Graphentheorie und ihre Anwendungen. Klett, 1974
[Trias] Trias Pairó, J.: Matemàtica discreta. Problemes resolts. Universitat Politècnica de Catalunya, 2009
[Wall] Wallis, W.D.: A beginner's guide to graph theory. Second edition. Birkhäuser, 2007
[Wall2] Wallis, W.D.: A beginner's guide to discrete mathematics. Second edition. Birkhäuser, 2012
[Wes] West, D.B.: Introduction to graph theory. Second edition. Prentice Hall, 2001
[Wil] Wilson, R.J.: Introduction to graph theory. Longman, 2010

Capítulo 20. Grafos eulerianos y hamiltonianos

El matemático suizo Leohnard EULER (1707–1783) resolvió en 1736 el llamado problema de los “puentes de Königsberg”: por la ciudad prusiana de Königsberg[1] discurre el río Pregel, formando en el centro de la ciudad de manera un tanto curiosa una pequeña isla, en donde se encontraba la catedral, entre otros edificios destacables. Esta isla estaba hasta 1945 unida a otras partes de la ciudad por siete puentes, como muestra la figura:



Se preguntaban los habitantes de Königsberg si sería posible dar un paseo por aquel entorno en el que se atravesara cada uno de los siete puentes una sola vez. La respuesta de Euler, que daremos en el transcurso de este capítulo, se considera el

[1] Ciudad anexionada a la Unión Soviética tras la segunda guerra mundial con el nombre de Kaliningrad, y definitivamente entregada por la República Federal de Alemania en los años sesenta.

ISBN: 978-84-17900-65-6

DOI: http://dx.doi.org/10.6035/Sapientia170

inicio de la teoría de grafos. La generalización del "agradable paseo" por el centro de la ciudad que se proponía en la pregunta originó la siguiente definición:

Definición. Un *camino euleriano* en un grafo G es una trayectoria que recorre cada arista exactamente una vez. Un *ciclo euleriano* es un camino euleriano cerrado. Un *grafo euleriano* es un grafo que contiene un ciclo euleriano.

Los grafos eulerianos se pueden clasificar fácilmente:

Teorema 20.1. *Sea G un grafo conexo. Son equivalentes:*

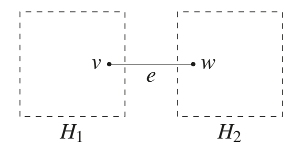
(a) *G es un grafo euleriano.*
(b) *Cada vértice de G posee grado par.*
(c) *G es unión de ciclos que tienen aristas disjuntas.*

(Dos subgrafos $G_1 = (V_1, E_1), G_2 = (V_2, E_2)$ de un grafo G se dice que tienen aristas disjuntas si $E_1 \cap E_2 = \varnothing$.)

Demostración.

$(a) \Rightarrow (b)$ En un camino euleriano cerrado, un vértice x se abandona tantas veces como se llega a él, lo que quiere decir que $\gamma(x)$ es par.

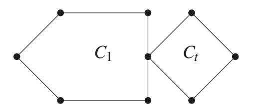
$(b) \Rightarrow (c)$ Supongamos que existe un puente e en G. Suprimiendo e, el grafo G descompone en dos componentes conexas:



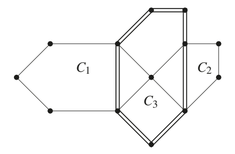
Por consiguiente, cada vértice en G_1 excepto a posee grado par en G_1, y a tiene grado impar en G_1 (ya que se eliminó una arista que incidía en a), lo que contradice (b).
Entonces existe un ciclo C_1 en G. Denotemos V_1 el conjunto de sus vértices y E_1 el de sus aristas. Eliminemos las aristas de C_1 del grafo G. Cada componente conexa de $G \setminus E_1$ que no sea un vértice aislado satisface la hipótesis de (b). En cada componente se elige de nuevo un ciclo y se repite el procedimiento anterior hasta que solamente queden vértices aislados. Los ciclos así obtenidos forman la descomposición buscada.

$(c) \Rightarrow (a)$ Sea $X = \bigcup_v C_v$. Existe un ciclo C_{v_1} que posee un vértice en común con C_1 (G es conexo):

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170



Así la unión $C_1 \cup C_{v_1}$ posee un camino euleriano. Por tanto, existe un ciclo C_{v_2} que interseca $C_1 \cup C_{v_1}$:



Se comienza por el punto de contacto a y se recorre primero $C_1 \cup C_{v_1}$, luego C_{v_2} y así sucesivamente.

□

El Teorema 20.1 asegura entonces que el problema de los puentes de Königsberg no es resoluble con un camino euleriano cerrado. ¿Lo será con uno abierto? Tampoco lo es, como garantiza el teorema siguiente:

Teorema 20.2. *Un grafo conexo G posee un camino euleriano abierto si y solamente si posee exactamente dos vértices a y b de grado impar. Cada uno de los caminos eulerianos abiertos que puede haber tiene entonces a y b por extremos.*

Demostración. Supongamos que G contiene un camino euleriano abierto con extremos a y b. Añadiendo otra arista entre a y b, obtenemos un grafo G' que contiene un camino euleriano cerrado. Por tanto, en G solamente los vértices a y b tendrán grado impar (cf. Teorema 20.1).

Recíprocamente, tras añadir una arista entre a y b, el grafo resultante G'' satisface la propiedad (2) del Teorema 20.1, por tanto, contiene un ciclo euleriano y así G contiene un camino euleriano abierto de extremos a y b. □

Lo que son las aristas a los caminos eulerianos, son los vértices a los caminos hamiltonianos:

Definición. Un *camino hamiltoniano* en un grafo G es un camino de G que recorre cada vértice una sola vez. Un *ciclo hamiltoniano* es un camino hamiltoniano cerrado. Un *grafo hamiltoniano* es un grafo que contiene un ciclo hamiltoniano.

Los grafos hamiltonianos reciben este nombre en honor a sir William Rowan Hamilton, matemático irlandés, que hacia 1870 ideó un juego que involucraba la

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

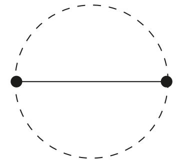
construcción de caminos de este tipo: dado un dodecaedro de madera, donde cada vértice representaba una ciudad, se trataba de recorrer todas las ciudades (yendo por las aristas) sin repetir y volviendo al punto de partida.

Para la existencia de caminos hamiltonianos las aristas múltiples no juegan, evidentemente, ningún papel. En lo que sigue se supondrá entonces que todos los grafos son simples.

Los caminos hamiltonianos son significativamente más difíciles de tratar que los eulerianos, y hasta la fecha no se conoce ningún criterio comparable al Teorema 20.1. Existen, empero, algunos resultados parciales que pasamos a discutir.

Teorema 20.3. *Un grafo hamiltoniano G no tiene ni puentes ni articulaciones.*

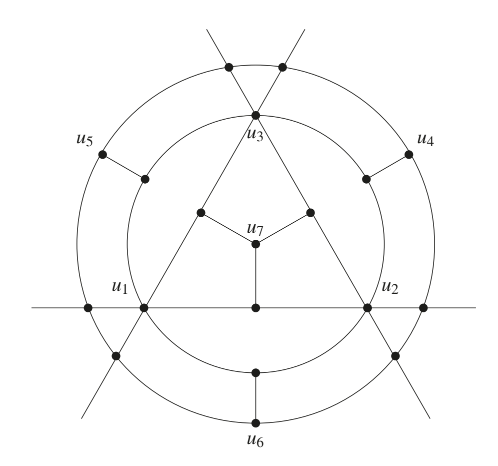
Demostración. Que no tiene articulaciones está claro. Además, observando se comprende fácilmente que cada arista está incluida en algún ciclo:



por tanto, G tampoco puede tener puentes. □

Una fuente de ejemplos para grafos que contienen ciclos hamiltonianos son los grafos completos: K_n contiene un ciclo hamiltoniano para todo $n \geq 3$. El grafo siguiente, por otro lado, muestra una forma de refutar la existencia de caminos o ciclos hamiltonianos en un grafo.

Ejemplo. El grafo siguiente posee 19 vértices y 33 aristas:



ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Un potencial camino hamiltoniano C para los 19 vértices necesita de 18 aristas. Ahora bien, ningún par de los vértices $u_1, u_2, \dots, u_7$ son adyacentes. Se tiene que

$$\gamma(u_1) = \gamma(u_2) = \gamma(u_3) = 6, \;\; \gamma(u_4) = \gamma(u_5) = \gamma(u_6) = \gamma(u_7) = 3.$$

Cada uno de estos vértices puede ser un extremo de a lo sumo dos aristas en el camino hamiltoniano C. Los otros pueden no ser tenidos en cuenta, es decir, por lo menos

$$3 \cdot 4 + 4 \cdot 1 = 16$$

aristas. Pero $33 - 16 = 17$ aristas no llegan para poder unir 19 vértices, pues se necesitan 18, lo que quiere decir que no puede existir un camino hamiltoniano en el grafo.

Algunas observaciones sencillas y útiles sobre grafos hamiltonianos son las siguientes:

(a) Un grafo con un vértice de grado 1 no puede ser hamiltoniano, pues en un ciclo hamiltoniano cada vértice es incidente con dos aristas del ciclo.
(b) Si $G = (V, E)$ tiene un ciclo hamiltoniano, entonces para $v \in V$ es $\gamma(v) \geq 2$.
(c) Si $v \in V$ y $\gamma(v) = 2$, entonces las dos aristas incidentes con el vértice v deben estar incluidas en cualquier ciclo hamiltoniano de G.
(d) Si $v \in V$ y $\gamma(v) > 2$, entonces al tratar de construir un ciclo hamiltoniano una vez que se ha pasado por el vértice v se dejan de tener en cuenta las aristas no utilizadas que son incidentes con v.
(e) Al construir un ciclo hamiltoniano para G no se puede obtener un ciclo para un subgrafo de G a menos que contenga todos los vértices de G.
(f) Si al quitar k vértices de un grafo G se produjeren más de k componentes conexas, entonces G no sería hamiltoniano; se deduce del hecho de que en un ciclo la anterior situación es imposible.

Veamos, sin demostración, el primer teorema profundo de este curso, debido al matemático húngaro Lajos PÓSA, nacido en 1947:

Teorema 20.4 (Pósa, 1962)**.** *Sea G un grafo con $|V(G)| = n \geq 3$. Supongamos que para cada número entero $r < \frac{n}{2}$ se verificara que el número de vértices a con $\gamma(a) \leq r$ es menor que r. Entonces el grafo G es hamiltoniano.*

Como corolarios se obtienen los dos resultados siguientes[2]:

Teorema 20.5 (Dirac, 1952)**.** *Sea G un grafo con $|V(G)| = n \geq 3$. Si $\gamma(a) \geq \frac{n}{2}$ para todo $a \in V$, entonces G es hamiltoniano.*

[2]Demostrados, respectivamente, por el físico inglés Paul Adrien Maurice DIRAC (1902–1984) y el matemático noruego ∅ystein ORE (1899–1968).

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Teorema 20.6 (Ore, 1960)**.** *Sea G un grafo con $|V(G)| = n \geq 3$. Si para cada par de vértices no adyacentes $a, b \in V$ se verifica la desigualdad*

$$\gamma(a) + \gamma(b) \geq n,$$

entonces G es hamiltoniano.

Omitimos la demostración de ambos resultados.

ISBN: 978-84-17900-65-6

DOI: http://dx.doi.org/10.6035/Sapientia170

[Bas] Basart i Muñoz, J.M.: Grafs: fonaments i algorismes. Universitat Autònoma de Barcelona, Servei de Publicacions, 1998

[Big] Biggs, N.L.: Discrete Mathematics. Second ed. Oxford U.P., 2004

[Cab] Caballero Roldán, Rafael et al.: Matemática Discreta para Informáticos. Ejercicios resueltos. Pearson/Prentice Hall, 2007

[Conr] Conradie, W., Goranko, V.: Logic and Discrete Mathematics. A concise introduction. Wiley, 2015

[FG] Ferrando, J.C., Gregori, V.: Matemática Discreta. 2. ed. Reverté, 2002

[Gall] Gallier, J.: Discrete Mathematics. Springer, 2011

[HHM] Harris, J.M., Hirst, J.L., Mossinghoff, M.J.: Combinatorics and Graph Theory. Second edition. Springer, 2010

[Laf] Laforest, Ch.: À la découverte des graphes et des algorithmes de graphes. EDP Sciences, 2017.

[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3. ed. McGraw Hill, 2007

[Ore] Ore, ∅.: Graphentheorie und ihre Anwendungen. Klett, 1974

[Trias] Trias Pairó, J.: Matemàtica discreta. Problemes resolts. Universitat Politècnica de Catalunya, 2009

[Wall] Wallis, W.D.: A beginner's guide to graph theory. Second edition. Birkhäuser, 2007

[Wall2] Wallis, W.D.: A beginner's guide to discrete mathematics. Second edition. Birkhäuser, 2012

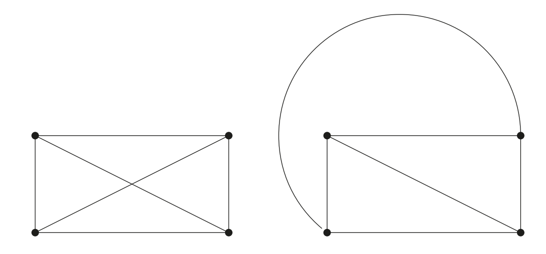
[Wes] West, D.B.: Introduction to graph theory. Second edition. Prentice Hall, 2001

[Wil] Wilson, R.J.: Introduction to graph theory. Longman, 2010

Capítulo 21. Grafos en el plano. Coloración

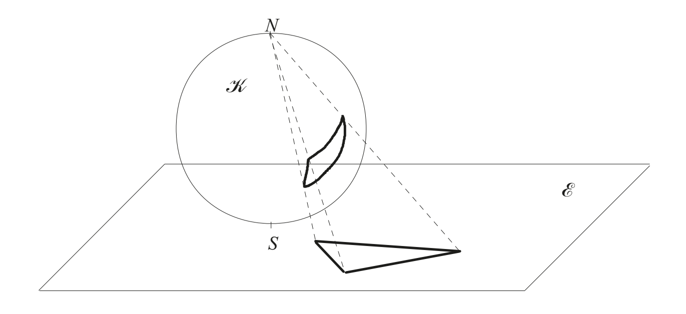
Un *grafo geométrico* en $\mathbb{R}^n$ es un conjunto V finito de puntos en $\mathbb{R}^n$ y de curvas lisas a trozos cuyos extremos pertenecen a V y que se cortan entre sí como mucho en sus extremos. Un grafo geométrico en $\mathbb{R}^2$ se llama *grafo plano*.

Un grafo se llama *planar* (o aplanable) si es isomorfo a un grafo plano. Por ejemplo, en la siguiente figura el grafo representado a la izquierda, aunque no es plano, es planar: véase su derecha.



En lo que sigue utilizaremos argumentos geométricos y topológicos de manera intuitiva, sin precisar los argumentos.

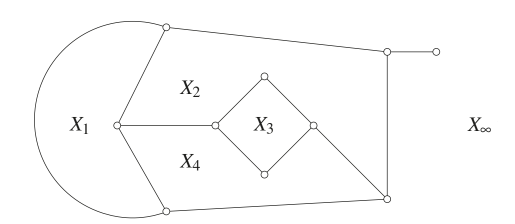
Un grafo es planar si y solamente si se puede "sumergir" (es decir, aplicar inyectivamente) en la superficie de la esfera. Para ello, resulta útil considerar la proyección estereográfica que establece una biyección entre los puntos de la superficie esférica $\mathscr{K}$, excepto el polo norte N y el plano $\mathscr{E}$, proyectando desde el polo norte:



El polo norte no estará contenido en ninguna arista.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Un grafo plano conexo G descompone el plano en un número finito de *dominios*:



El *borde* de un dominio es el subgrafo de todos los vértices y aristas que lo tocan.

Entre el número de vértices, aristas y dominios de un grafo plano conexo existe una interesante relación:

Teorema 21.1 (Formula de Euler)**.** *Sea $G = (V,E)$ un grafo plano conexo que posee g dominios. Entonces*

$$|V| - |E| + g = 2.$$

Demostración. Se demuestra por inducción sobre g. Para $g = 1$, X no contiene ciclos, y al ser conexo, es un árbol, luego $|V| = |E| + 2 - 1 = |E| + 1$. Supongamos ahora la afirmación cierta para todos los grafos con $g - 1 \geq 1$ dominios. Sea X un grafo plano conexo con g dominios. Separando de X una arista e que esté en un ciclo, es claro que $X \setminus \{e\}$ es plano, con $g - 1$ dominios, y aplicando la hipótesis de inducción queda

$$|V| - (|E| - 1) + (g - 1) = 2.$$

□

El Teorema 21.1 permite demostrar algunas propiedades de los grafos planares:

Teorema 21.2. *Sea $G = (V,E)$ un grafo plano conexo, entonces $|V| \geq 3$.*

(a) *Si el borde de cada dominio es un ciclo de longitud como poco n, entonces*

$$|E| \leq \frac{n(|V| - 2)}{n - 2} \quad (n \geq 3)$$

(b) *Se tiene que $|E| \leq 3|V| - 6$.*

(c) *X tiene por lo menos 3 vértices, cuyo grado es ≤ 5.*

Demostración. Se omite. □

ISBN: 978-84-17900-65-6 DOI: http://dx.doi.org/10.6035/Sapientia170

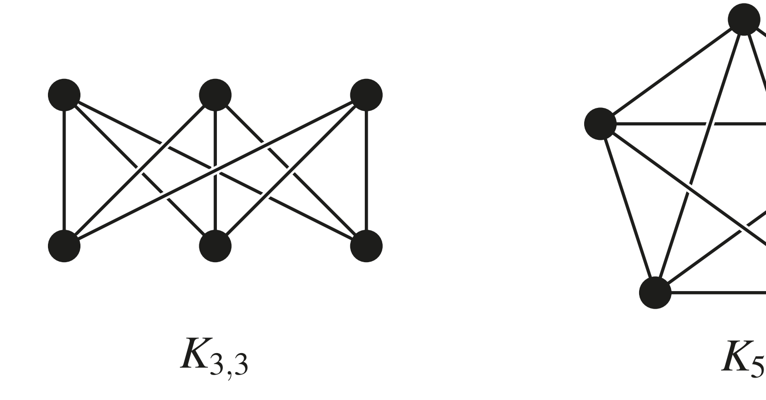
Definición. Sea G un grafo. Su *grafo complementario* $\overline{G}$ es aquel grafo que tiene por vértices los vértices de G y por aristas aquellas que conectan vértices que no están unidos mediante aristas en el grafo G.

Teorema 21.3. *Sea* $G = (V,E)$ *un grafo con* $|V| \geq 11$. *Si G es planar, entonces su complementario* $\overline{G}$ *no lo es.*

Demostración. Se omite. □

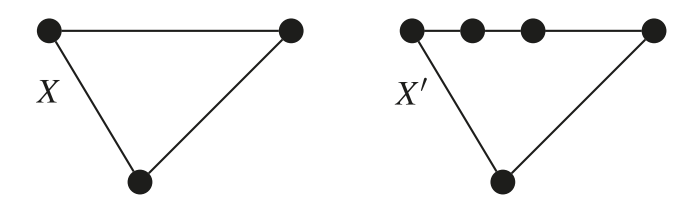
Queremos usar los resultados probados para mostrar que los grafos K_5 y $K_{3,3}$ no son planares.

En lo concerniente al grafo K_5 se tiene que $|V| = 5$, $|E| = \binom{5}{2} = 10$, es simple, conexo y además $10 \not\leq 3 \cdot 5 - 6 = 9$, por lo que no es planar de acuerdo con el Teorema 21.2.



En cuanto al grafo $K_{3,3}$, si fuera planar, tendría que tener $g = 2 - 6 + 9 = 5$ dominios. Por otro lado, cada ciclo en $K_{3,3}$ tiene longitud ≥ 4 (cada arista toca a lo sumo dos dominios), por lo que se tiene que $4g \leq 2g$, contradicción.

Un grafo X' se dice que es una *subdivisión* de X si X' se forma añadiendo nuevos vértices en las aristas de X:



ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Sin demostración enunciamos la siguiente caracterización de los grafos planares, probada en 1930 por el polaco Kazimierz KURATOWSKI (1896–1980):

Teorema 21.4 (Teorema de KURATOWSKI)**.** *Un grafo X es planar si y solamente si no contiene como subgrafos ninguna subdivisión de $K_{3,3}$ ó K_5.*

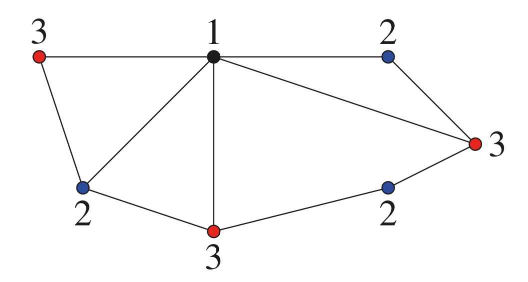
Terminamos la introducción a la teoría de grafos de este curso con un último concepto importante.

Definición. Una coloración (de los vértices) del grafo $G = (V,E)$ con m colores es una aplicación $f : V \to \{1,\dots,m\}$ tal que cualesquiera dos vértices adyacentes están coloreados de manera diferente. El menor m para el que existe una coloración permitida de G con m colores se llama número cromático de G. Se denota $\chi(G)$. Si $\chi(G) = m$ entonces G se dice *m-cromático*. En el caso en que $\chi(G) \leq m$, entonces G se llama *m-coloreable*.

Obsérvese que una m-coloración, esto es, una coloración $f : V \to \{1,\dots,m\}$, no es más que una partición del conjunto de vértices V del grafo en m subconjuntos de V. Por ejemplo, los grafos 1-coloreables no triviales son los grafos sin aristas; los grafos 2-coloreables no triviales con $\chi(G) = 2$ son exactamente los grafos bipartitos que posean al menos una arista.

Los conjuntos $f^{-1}(n)$, $n \in \{1,\dots,m\}$ se denominan clases de colores de la coloración f.

Ejemplo. (1) El grafo de la figura siguiente posee número cromático 3. Además, si f es la coloración, es decir, $f : V \to \{1,2,3\}$, la clase de color $f^{-1}(1)$ está formada por el vértice negro, en tanto que las clases de colores $f^{-1}(2)$ y $f^{-1}(3)$ poseen los tres vértices azules y rojos, respectivamente:



(2) La elaboración de un horario de clases se puede ver como un problema de coloreabilidad de un grafo: los vértices corresponden a las horas en las que se imparte una determinada clase. Dos clases estarán unidas por una arista si y solamente si

no pueden tener lugar al mismo tiempo. Una coloración se corresponde entonces con un horario en el que no hay colisiones de clases.

(3) Grupos de trabajo: Si $A_1, A_2, \ldots, A_r$ denotan los grupos de trabajo, y $O_1, \ldots, O_s$ son obras, no se quiere que ningún grupo trabaje en varias obras al mismo tiempo. Dos grupos no pueden trabajar al mismo tiempo en una obra. Así, los vértices del grafo los forman los pares (A_i, O_j) para los que el grupo de trabajo A_i es adecuado para la obra O_j. Por tanto

$$\{(A_i, O_j), (A_k, O_\ell)\} \in E \quad \Longleftrightarrow \quad i = k \text{ ó } j = \ell.$$

Una coloración de este grafo se corresponde con el número de fechas tales que todas las obras se puedan efectuar sin verse afectados porque otras obras hayan de realizarse al mismo tiempo.

La propiedad de coloración ayuda a responder la pregunta de cuántas citas han de concertarse por lo menos para que todas las obras puedan llevarse a cabo.

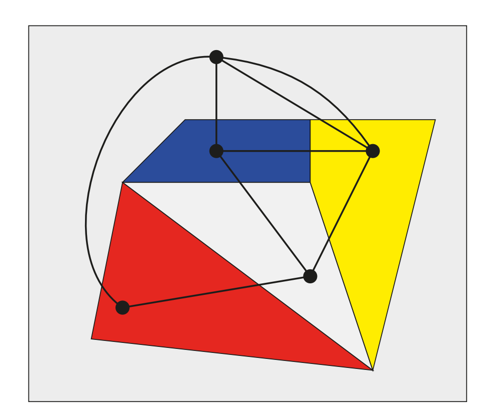
Teorema 21.5. *Con la notación anterior, se verifica que:*

$$\chi(G) \leq 1 + \max_{G' \subseteq G} \left(\min_{x \in V(G')} \gamma_G(x) \right) \leq 1 + \max_{x \in V} \gamma(x).$$

Demostración. Más o menos complicada por inducción sobre $\chi(G)$. □

Como los grafos completos K_n muestran, las cotas del teorema anterior no se pueden mejorar.

Una aplicación clásica de esta teoría es la coloración de mapas políticos de países. Dado un mapa, podemos formar un grafo asignando a cada país un vértice; dos vértices estarán unidos por una arista si y solamente si los correspondientes países poseen una frontera común.



ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Evidentemente, de esta manera se obtiene un grafo planar. Una coloración del grafo corresponde a una coloración del mapa en la que los países vecinos reciben distintos colores. Un teorema que fue difícil de resolver —y cuya demostración fue efectuada en última instancia por ordenador, lo que no estuvo exento de polémica— fue el que afirma que cuatro colores bastan:

Teorema 21.6 (Teorema de los 4 colores)**.** *Todo grafo planar G admite una coloración con 4 colores; esto es,* $\chi(G) \leq 4$.

Fue planteado en 1852 por un estudiante sudafricano de A. de Morgan, matemático y botánico, llamado Francis GUTHRIE (1831–1899). El Teorema de los cuatro colores fue probado con ayuda de un ordenador por el matemático estadounidense Kenneth APPEL (1932–2013) junto con el alemán Wolfgang HAKEN (nacido en 1928). El matemático británico Percy John HEAWOOD (1861–1955) había demostrado ya en 1890 que bastan cinco colores:

Teorema 21.7 (Teorema de los 5 colores)**.** *Para todo grafo planar G es 5-coloreable; es decir, se tiene que* $\chi(G) \leq 5$.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

[Bas] Basart i Muñoz, J.M.: Grafs: fonaments i algorismes. Universitat Autònoma de Barcelona, Servei de Publicacions, 1998

[Big] Biggs, N.L.: Discrete Mathematics. Second ed. Oxford U.P., 2004

[Cab] Caballero Roldán, Rafael et al.: Matemática Discreta para Informáticos. Ejercicios resueltos. Pearson/Prentice Hall, 2007

[Conr] Conradie, W., Goranko, V.: Logic and Discrete Mathematics. A concise introduction. Wiley, 2015

[FG] Ferrando, J.C., Gregori, V.: Matemática Discreta. 2. ed. Reverté, 2002

[Gall] Gallier, J.: Discrete Mathematics. Springer, 2011

[HHM] Harris, J.M., Hirst, J.L., Mossinghoff, M.J.: Combinatorics and Graph Theory. Second edition. Springer, 2010

[Laf] Laforest, Ch.: À la découverte des graphes et des algorithmes de graphes. EDP Sciences, 2017.

[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3. ed. McGraw Hill, 2007

[Ore] Ore, ∅.: Graphentheorie und ihre Anwendungen. Klett, 1974

[Trias] Trias Pairó, J.: Matemàtica discreta. Problemes resolts. Universitat Politècnica de Catalunya, 2009

[Wall] Wallis, W.D.: A beginner's guide to graph theory. Second edition. Birkhäuser, 2007

[Wall2] Wallis, W.D.: A beginner's guide to discrete mathematics. Second edition. Birkhäuser, 2012

[Wes] West, D.B.: Introduction to graph theory. Second edition. Prentice Hall, 2001

[Wil] Wilson, R.J.: Introduction to graph theory. Longman, 2010

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

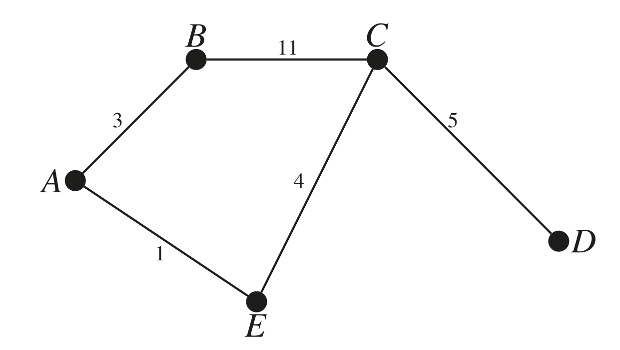
Capítulo 22.
Grafos y distancias

Se consideran unas ciudades $A_1, A_2, \ldots, A_n$ unidas entre sí por carreteras y se desea calcular la distancia mínima (y el recorrido correspondiente) de A_1 a algún A_i. Evidentemente se puede expresar el problema mediante un grafo cuyos vértices representan las ciudades y cuyas aristas representan las carreteras. Ahora bien, ¿cómo representar las distancias entre las ciudades?

Para tratar problemas de esta naturaleza generalizamos el concepto de grafo asociando a cada arista un peso o distancia; se habla entonces de grafo pesado:

Definición. Un *grafo pesado* (o *ponderado*) es un grafo $G = (V, E)$ junto con una aplicación (peso o distancia) $w : E \to \mathbb{R}_{\geq 0}$.

Como en los capítulos anteriores, nuestro estudio se restringe a grafos simples, a menos que se indique lo contrario. Un ejemplo de representación de un grafo pesado es:



Seguimos introduciendo un poco de terminología. Sea G un grafo pesado. Dada una arista a de G, el *peso de* a es su imagen por w, es decir, $w(a)$. Dada una trayectoria $x_0, x_1, \ldots, x_n$ su peso (o distancia) es la suma

$$\sum_{i=0}^{n-1} w(\{x_i, x_{i+1}\}).$$

ISBN: 978-84-17900-65-6

DOI: http://dx.doi.org/10.6035/Sapientia170

Además, dados $x, y \in V$, la distancia de x a y es

$$d(x,y) = \min\{\text{pesos de trayectorias de } x \text{ a } y\}$$

(o bien $d(x,y) = \infty$ si x e y están en distintas componentes conexas).

Volvemos a la pregunta inicial: ¿Cómo encontrar el camino de peso mínimo de vértice fijado, digamos x, a todos los demás? La respuesta nos la da el *algoritmo de Dijkstra*.

Algoritmo de Dijkstra[1] con base en un vértice x:

Sea $G = (V,E)$ un grafo (simple). Dados $x, y \in V$, denotamos por $w(x,y)$ al peso de la única arista de x a y, si existe; si no existe, escribiremos $w(x,y) = \infty$.

Hay tantas etapas como vértices en la componente conexa de x.

En cada etapa se van a tener unos vértices con etiqueta permanente (P_i) y otros con etiqueta temporal (T_i) de forma que $V = P_i \cup T_i$ (unión disjunta). La etiqueta permanente va a ser la distancia y no cambia en las sucesivas etapas; la etiqueta temporal es una aproximación y puede disminuir:

$$P_i = P_{i-1} \cup \{v_i\} \quad T_i = T_{i-1} \setminus \{v_i\}.$$

Comenzamos el algoritmo:

Primera etapa: $v_1 := x$, $P_1 := \{v_1\}$, $T_1 := V \setminus P_1$, $p(v_1) := 0$, $t_1(z) := w(x,z)$ para todo $z \in T_1$. Denotemos por C_{v_1} el camino (simple, de longitud 0) $x = v_1$.

Etapa i: Se tienen, de la etapa anterior
P_{i-1} con etiqueta permanente $p(z)$
T_{i-1} con etiqueta temporal $t_{i-1}(z)$.

Entonces se elige $v_i \in T_{i-1}$ tal que

$$t_{i-1}(v_i) = \min\{t_{i-1}(z) : z \in T_{i-1}\}$$

y finita (si existe); y se hace

$$P_i = P_{i-1} \cup \{v_i\} \quad T_i = T_{i-1} \setminus \{v_i\}. p(v_i) = t_{i-1}(v_i).$$

Si $z \in T_i$, entonces

$$t_i(z) = \min\{t_{i-1}(z), p(v_i) + w(v_i,z)\}.$$

[1]Por el informático holandés Edsger W. DIJKSTRA (1930–2002).

Sea ℓ mínimo tal que $p(v_i) = t_\ell(v_i)$ (es decir, $t_{\ell-1}(v_i) > p(v_i)$.) Entonces

$$C_{v_i} : C_{v_\ell}, v_i.$$

Salida: En la etapa n se obtiene o bien $T_n = \varnothing$ o bien $t_n(z) = \infty$ para todo $z \in T_n$, lo que permite concluir:
P_n son los vértices de la componente conexa de x;
$p(v) = d(x,v)$ para todo $v \in P_n$;
C_v es un camino de mínima distancia de x a v.

Que el algoritmo efectivamente funciona se justifica con los dos resultados siguientes, que no vamos a demostrar:

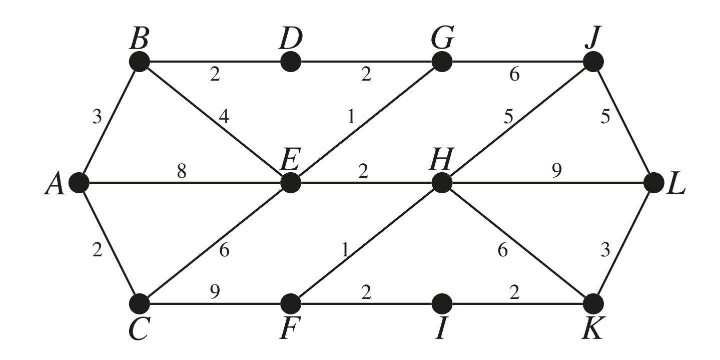
Teorema 22.1. *Al finalizar el algoritmo, P_n es el conjunto de vértices de la componente conexa de x en G, y para todo $z \in P_n$, C_z es un camino de x a z.*

(Téngase en cuenta que si $t_i(z) = \infty$, entonces z no es adyacente a ningún vértice de P_i.) Dados $S \subseteq V$ y $z \in V \subseteq S$, diremos que un camino en G une directamente S con z si el vértice que precede en el camino a z pertenece a S.

Teorema 22.2. *Se tiene que:*

(a) *Para todo $z \in P_n$, $d(x,z) = p(z)$.*
(b) *Para todo $i \geq 1$ y todo $z \in T_i$, $t_i(z)$ es el peso de un camino de peso mínimo entre aquellos que unen directamente P_i con z.*
(c) *Para todo $z \in P_n$, C_z es un camino de peso mínimo entre x y z.*

Ejemplo. Calculemos el camino de distancia mínima del vértice A al vértice L en el grafo siguiente:



Para aplicar el algoritmo construimos una tabla con $n+2$ columnas (siendo $n = |V(G)|$) y tantas filas como etapas tiene el algoritmo:

Elementos de matemática discreta
ISBN: 978-84-17900-65-6

Julio José Moyano Fernández
DOI: http://dx.doi.org/10.6035/Sapientia170

◇ en la columna 0 se van anotando los vértices que pasan a ser permanentes;
◇ en la columna $n+1$ se van escribiendo los caminos C_{v_i};
◇ cada una de las columnas $1, 2, \ldots n$ corresponde a un vértice del grafo.

Respecto a las filas, contienen la siguiente información:

Primera fila:

◇ el vértice permanente es v_1;
◇ para $1 \leq i \leq n$, en la columna i se escribe

$$w(v_1, z) = t_1(z)$$

si z es el vértice correspondiente a la columna;
◇ en la columna $n+1$ se anota el camino $C_{v_1} = v_1$.

Fila i-ésima:

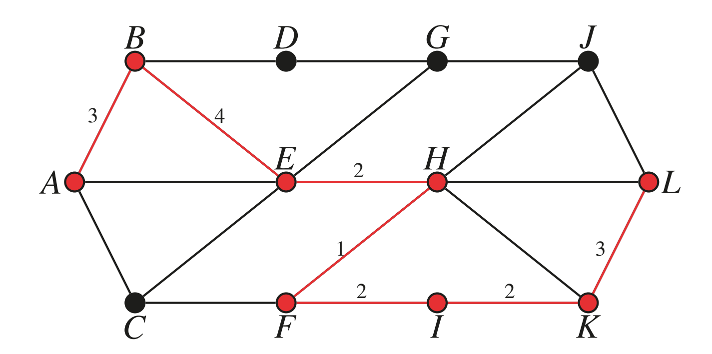
◇ en la columna 0 se escribe el vértice v_i (el que corresponde a ser permanente en esa etapa);
◇ en la columna j se escribe $t_i(z)$ si z es el vértice de la columna;
◇ en la columna $n+1$ se anota el camino C_{v_i}.

Para el ejemplo que nos ocupa se obtiene la siguiente tabla:

	A	B	C	D	E	F	G	H	I	J	K	L	C_{v_i}
A	–	3	**2**	∞	8	∞	∞	∞	∞	∞	∞	∞	A
C	–	**3**	–	∞	8	11	∞	∞	∞	∞	∞	∞	AC
B	–	–	–	**5**	7	11	∞	∞	∞	∞	∞	∞	AB
D	–	–	–	–	**7**	11	7	∞	∞	∞	∞	∞	ABD
E	–	–	–	–	–	11	**7**	9	∞	∞	∞	∞	ABE
G	–	–	–	–	–	11	–	**9**	∞	13	∞	∞	$ABDG$
H	–	–	–	–	–	**10**	–	–	∞	13	15	18	$ABEH$
F	–	–	–	–	–	–	–	–	**12**	13	15	18	$ABEHF$
I	–	–	–	–	–	–	–	–	–	**13**	14	18	$ABEHFI$
J	–	–	–	–	–	–	–	–	–	–	**14**	18	$ABDGJ$
K	–	–	–	–	–	–	–	–	–	–	–	**17**	$ABEHFIK$
L	–	–	–	–	–	–	–	–	–	–	–	–	$ABEHFIKL$

El camino de distancia mínima de A a L es el camino $ABEHFIKL$, y la distancia mínima es 17:

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

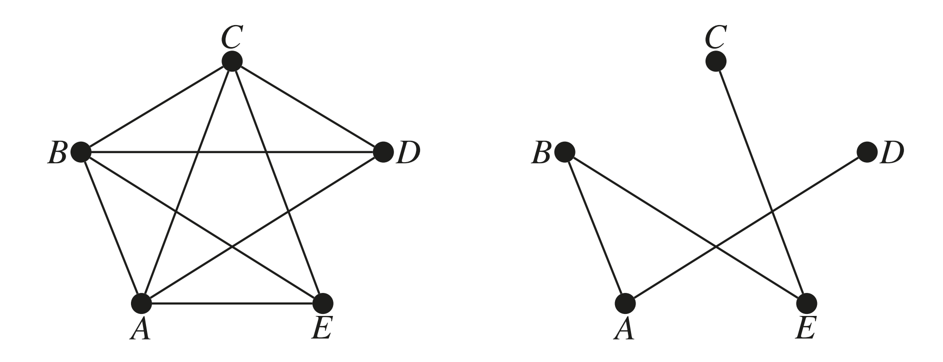


Una descripción tabular del algoritmo de Dijkstra parecida a la expuesta se puede encontrar en [**Lop**].

Los grafos pesados también juegan un papel esencial en la minimización de costes. Por ejemplo, supongamos que queremos construir una red de carreteras que una 5 ciudades, digamos A,B,C,D y E, entre sí, con coste mínimo. El coste de unir dos ciudades está dado por la siguiente matriz:

	A	B	C	D	E
A	0	3	5	11	9
B	3	0	3	9	8
C	5	3	0	∞	10
D	11	9	∞	0	7
E	9	8	10	7	0

La situación se representa en un grafo pesado G:



Grafo G y subgrafo generador de G.

Se trata de encontrar un subgrafo H (el de las carreteras que se construyen), con las características siguientes:

(1) $V(H) = V(G)$, es decir, H es subgrafo *generador* de G;
(2) H es conexo;
(3) H no contiene ciclos;
(4) el peso $w(H) = \sum_{e \in E(H)} w(e)$ mínimo posible.

Las características (2) y (3) son la definición de árbol. El problema es, pues, encontrar un árbol generador T del grafo G de peso mínimo (es decir, tal que si T' es otro árbol generador, entonces $w(T) \leq w(T')$). La pregunta es: ¿Existe siempre un árbol generador de peso mínimo de un grafo pesado?

Evidentemente, si existe un árbol generador, G es conexo (por definición de árbol). Además, el recíproco también es cierto. De hecho, el siguiente algoritmo nos da una forma de encontrar *un* (y no decimos *el*, porque no hay unicidad en la salida) árbol generador de peso mínimo, dado un grafo pesado conexo:

Algoritmo de Kruskal[2]

Entrada: Grafo G pesado, conexo.

Inicialización: Sea H_0 el subgrafo generador de G con $E(H_0) = \varnothing$.

Etapa i-ésima: Si H_{i-1} no es conexo, sea e_i una arista de peso mínimo entre todas las que unen dos componentes distintas de H_{i-1}. Sea H_i el subgrafo generador de G con aristas $E(H_i) = E(H_{i-1}) \cup \{e_i\}$.

Salida: El algoritmo finaliza cuando se encuentra H_k conexo. La salida es H_k.

El algoritmo funciona, de acuerdo con los dos resultados siguientes (que no vamos a demostrar):

Teorema 22.3. *Sea $n = |V(G)|$. Para $0 \leq i \leq k$, el grafo H_i es un bosque con $n-i$ componentes conexas. En particular, $k = n-1$ y la salida del algoritmo, H_{n-1}, es un árbol generador.*

Además, el output es de peso mínimo:

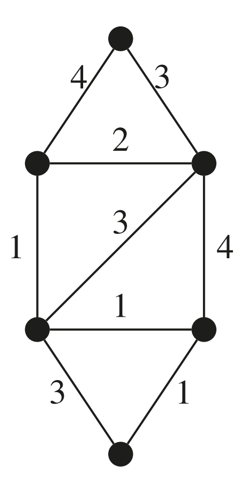
Teorema 22.4. *Sea T un árbol generador de G. Supongamos que $E(T) = \{b_1, \ldots, b_{n-1}\}$ con $w(b_i) \leq w(b_2) \leq \ldots \leq w(b_{n-1})$. Entonces, $w(a_i) \leq w(b_i)$ para $1 \leq i \leq n-1$.*

[2]Por el matemático estadounidense Joseph B. KRUSKAL (1928–2010).

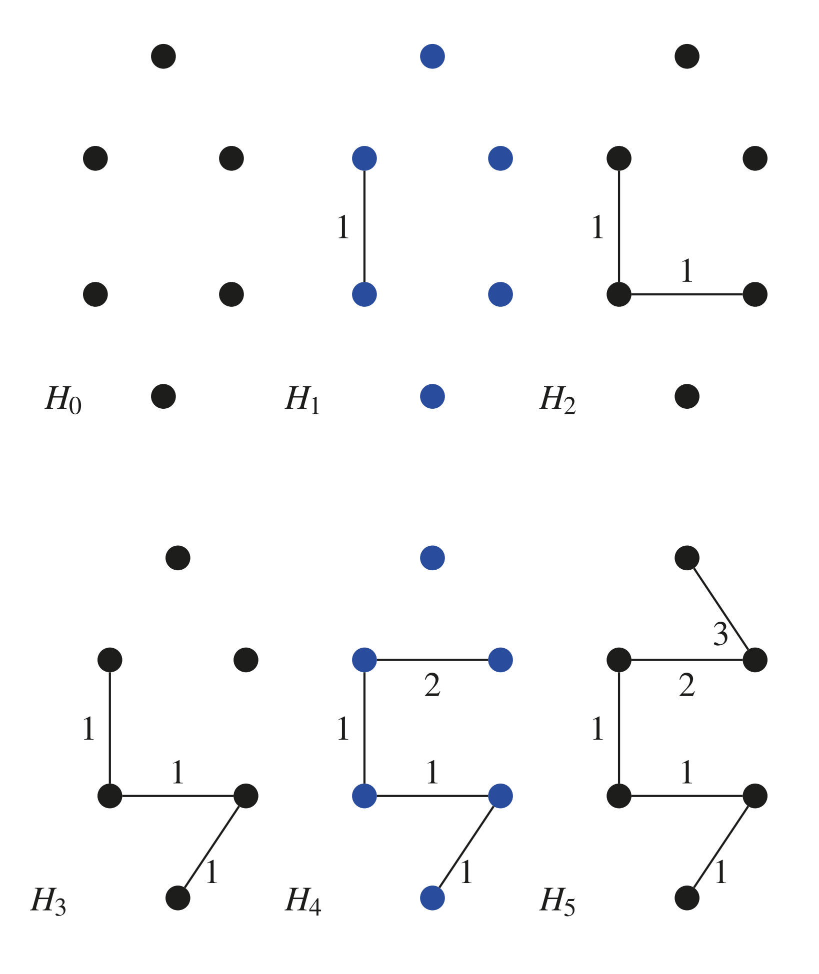
ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

Terminemos el capítulo con un ejemplo de aplicación del algoritmo de Kruskal.

Ejemplo. Consideremos el siguiente grafo pesado G:



De acuerdo con las explicaciones anteriores, el algoritmo de Kruskal distingue las siguientes etapas para G:



ISBN: 978-84-17900-65-6

DOI: http://dx.doi.org/10.6035/Sapientia170

Efectivamente, el grafo H_5 es un árbol generador para el grafo de partida G y, por construcción, es de peso mínimo

$$1+1+1+2+3=8.$$

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

[Bas] Basart i Muñoz, J.M.: Grafs: fonaments i algorismes. Universitat Autònoma de Barcelona, Servei de Publicacions, 1998

[Bh] Bhargava, A.Y.: Algoritmos, Anaya, 2018

[Big] Biggs, N.L.: Discrete Mathematics. Second ed. Oxford U.P., 2004

[Cab] Caballero Roldán, Rafael et al.: Matemática Discreta para Informáticos. Ejercicios resueltos. Pearson/Prentice Hall, 2007

[Conr] Conradie, W., Goranko, V.: Logic and Discrete Mathematics. A concise introduction. Wiley, 2015

[HHM] Harris, J.M., Hirst, J.L., Mossinghoff, M.J.: Combinatorics and Graph Theory. Second edition. Springer, 2010

[Laf] Laforest, Ch.: À la découverte des graphes et des algorithmes de graphes. EDP Sciences, 2017.

[Lip] Lipschutz, S., Lipson, M.L.: Matemáticas Discretas. 3. ed. McGraw Hill, 2007

[Ore] Ore, ∅.: Graphentheorie und ihre Anwendungen. Klett, 1974

[Trias] Trias Pairó, J.: Matemàtica discreta. Problemes resolts. Universitat Politècnica de Catalunya, 2009

[Wall] Wallis, W.D.: A beginner's guide to graph theory. Second edition. Birkhäuser, 2007

[Wes] West, D.B.: Introduction to graph theory. Second edition. Prentice Hall, 2001

[Wil] Wilson, R.J.: Introduction to graph theory. Longman, 2010

Bibliografía

[Aig] Aigner, M. (2007): A course in enumeration. Springer, Berlin.
[Ant] Antoine, R., Camps, R., Moncasi, J. (2007): Introducció a l'àlgebra abstracta. Universitat Autònoma de Barcelona, Barcelona.
[Art] Artin, M. (1993): Algebra. Birkhäuser, Basel.
[Bas] Basart i Muñoz, J.M.: Grafs: fonaments i algorismes. Universitat Autònoma de Barcelona, Servei de Publicacions, 1998
[BRV] Basart, J. M., Rifà, J., Villanueva, M. (1999): Fonaments de matemàtica discreta. Elements de combinatòria i d'aritmètica. Universitat Autònoma de Barcelona, Barcelona.
[BT] Beutelspacher, A., Törner, G. (2015): Interview mit Professor Dr. Günter Pickert. Mitteilungen der DMV, 23 (1), 48–58.
[Bh] Bhargava, A.Y. (2018): Algoritmos, Anaya, Madrid.
[Big] Biggs, N.L. (2004): Discrete Mathematics. Second ed. Oxford U.P., Oxford.
[Bord] Bordes Solanas, M. (2016): Las trampas de circe: falacias lógicas y argumentación informal. Cátedra, Madrid.
[Bre] Brenner, H. (2012): Mathematik für Anwender I, Skript, Osnabrück WS 2011/12, Osnabrück.
[Bru] Bruns, W. (2012): Lineare Algebra 1, Skript, Osnabrück WS 2011/12, Osnabrück.
[Cab] Caballero Roldán, R. et al. (2007): Matemática Discreta para Informáticos. Ejercicios resueltos. Pearson/Prentice Hall, Madrid.
[Carr] Carroll, L. (2015): El juego de la lógica. Alianza, Madrid.
[Conr] Conradie, W., Goranko, V. (2015): Logic and Discrete Mathematics. A concise introduction. Wiley, West Sussex.
[Dox] Doxiadis, A, Papadimitriou, Ch. (2009): Logicomix. An epic search for truth. Bloomsbury, New York.
[EG] Eriksson, K., Gavel, H. (2013): Diskret matematik och diskreta modeller. Studenlitteratur, Lund.
[E] Evnin, A. Yú. (2015): Emparejamientos en grafos bipartitos: en torno al Teorema de Hall. HAYKA, Moscú.
[Farr] Farré, R. et al. (2011): Lógica para informáticos. Marcombo, Barcelona.
[FG] Ferrando, J.C., Gregori, V. (2002): Matemática Discreta. 2. ed. Reverté, Barcelona.
[Fine] Fine, B. et al. (2018): Geometry and discrete mathematics. De Gruyter, Berlin/Boston.
[FEA] Franco, J.R., Espinel, M.C., Almeida, P.R. (2008): Manual de combinatoria. Abecedario, Badajoz.

[GOV] Galindo Pastor, C., Orús Báguena, M.P., Vindel Cañas, M.P. (1997): Problemes de matemàtica discreta. Universitat Jaume I, Castelló de la Plana.
[Gall] Gallier, J. (2011): Discrete Mathematics. Springer, New York.
[Galli] Gallinari, A. (2009): Apuntes y problemas de lógica matemática. Universidad Rey Juan Carlos, Madrid.
[Gr] Grimaldi, R.P. (1989): Matemáticas discreta y combinatoria. Addison-Wesley Iberoamericana, México.
[Ham] Hamilton, A.G. (1978): Logic for mathematicians, Cambridge U.P., Cambridge.
[HHM] Harris, J.M., Hirst, J.L., Mossinghoff, M.J. (2010): Combinatorics and Graph Theory. Second edition. Springer, New York.
[Hasenj] Hasenjaeger, G. (1968): Conceptos y problemas de la lógica moderna. Labor, Barcelona.
[KN] Kumke, S.O., Noltemeier, H. (2009): Graphentheoretische Konzepte und Algorithmen. Vieweg+Teubner, Wiesbaden.
[KR] Krischke, A., Röpcke, H. (2015): Graphen und Netzwerktheorie. Hanser, Leipzig.
[Laf] Laforest, Ch. (2017): À la découverte des graphes et des algorithmes de graphes. EDP Sciences, France.
[LiPi] Lidl, R., Pilz, G. (1998): Applied Abstract Algebra. Second edition. Springer, New York.
[Lip] Lipschutz, S., Lipson, M.L. (2007): Matemáticas Discretas. 3. ed. McGraw Hill, México.
[Lop] López Ortí, J.A. (2010): Métodos matemáticos, Universitat Jaume I, Colección Sapientia 41, Castelló de la Plana.
[Mar] Martin, G.E. (2001): Counting: the art of enumerative combinatorics. Springer, New York.
[Moy] Moyano-Fernández, J.J. (2013): Mathematik für Anwender I, Skript, Osnabrück SS 2012/13, Osnabrück.
[Ore] Ore, ∅. (1974): Graphentheorie und ihre Anwendungen. Klett, Stuttgart.
[Pla] Pla i Carrera, J. (2006): Introducció a la metodologia de la Matemàtica. Universitat de Barcelona, Barcelona.
[PTW] Pólya, G., Tarjan, R.E., Woods, D.R. (2010): Notes on introductory combinatorics. Birkhäuser, Boston.
[Pur] Purkert, W., Ilgauds, H.J. (1987): Georg Cantor. Vita Mathematica, Birkhäuser, Basel/Boston/Stuttgart.
[Quine1] Quine, W.V. (1966): Selected logic papers. Random House, New York.
[Quine2] Quine, W.V. (1966): Methods of logic. Routledge and Kegan Paul, London.
[Rib]Ríbnikov, K. (1988): Análisis combinatorio. Mir, Moscú.
[Rios] Ríos, S. (1974): Matemática finita. Paraninfo, Madrid.
[SS] Sanz-Serna, J.M. (1998): Diez lecciones de cálculo numérico. Universidad de Valladolid, Valladolid.
[SchWie] Schafmeister, O., Wiebe, H. (1978): Grundzüge der Algebra. B.G. Teubner, Stuttgart.
[Smull] Smullyan, R.M. (2014): A Beginner's guide to Mathematical Logic. Dover, Mineola/New York.

ISBN: 978-84-17900-65-6
DOI: http://dx.doi.org/10.6035/Sapientia170

[StW] Storch, U. und Wiebe, H. (1999): Lehrbuch der Mathematik, Band 2. Spektrum, Heidelberg.

[Trias] Trias Pairó, J. (2009): Matemàtica discreta. Problemes resolts. Universitat Politècnica de Catalunya, Barcelona.

[Wall] Wallis, W.D. (2007): A beginner's guide to graph theory. Second edition. Birkhäuser, Boston.

[Wall2] Wallis, W.D. (2012): A beginner's guide to discrete mathematics. Second edition. Birkhäuser, Boston.

[Wes] West, D.B. (2001): Introduction to graph theory. Second edition. Prentice Hall, New Jersey.

[Wil] Wilson, R.J. (2010): Introduction to graph theory. Longman, Harlow.